

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT				1. CONTRACT ID CODE J		PAGE 1 OF 2 PAGES	
2. AMENDMENT/MODIFICATION NUMBER 0003		3. EFFECTIVE DATE 23 JAN 2026		4. REQUISITION/PURCHASE REQUISITION NUMBER		5. PROJECT NUMBER (If applicable) 512203	
6. ISSUED BY W076 ENDIST TULSA KO CONTRACTING DIVISION, 2488 E 81ST STREET TULSA, OK 74137-4290 UNITED STATES MELISSA HYSLOP, EMAIL: MELISSA.D.HYSLOP@USACE.ARMY.MIL TELEPHONE: (918)669-7670		CODE W912BV		7. ADMINISTERED BY (If other than Item 6) SCD: PAS:		CODE	
8. NAME AND ADDRESS OF CONTRACTOR (Number, street, county, State and ZIP Code)				(X)		9A. AMENDMENT OF SOLICITATION NUMBER W912BV26RA004	
				(X)		9B. DATED (SEE ITEM 11) 11 DEC 2025	
				()		10A. MODIFICATION OF CONTRACT/ORDER NUMBER	
				()		10B. DATED (SEE ITEM 13)	
CODE		FACILITY CODE					

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

☒ The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers ☒ is extended. ☐ is not extended.

Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods:
 (a) By completing items 8 and 15, and returning 1 copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted;
 or (c) By separate letter or electronic communication which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER.
 If by virtue of this amendment you desire to change an offer already submitted, such change may be made by letter or electronic communication, provided each letter or electronic communication makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.

12. ACCOUNTING AND APPROPRIATION DATA (If required)
 SEE SECTION G - CONTRACT ADMINISTRATION DATA

**13. THIS ITEM APPLIES ONLY TO MODIFICATIONS OF CONTRACTS/ORDERS.
IT MODIFIES THE CONTRACT/ORDER NUMBER AS DESCRIBED IN ITEM 14.**

CHECK ONE	A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: (Specify authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NUMBER IN ITEM 10A.
☐	
☐	B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (such as changes in paying office, appropriation data, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b).
☐	C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF:
☐	D. OTHER (Specify type of modification and authority)

E. IMPORTANT: Contractor ☐ is not ☐ is required to sign this document and return _____ copies to the issuing office.

14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.)

Amendment 0003 is hereby issued to provide the updated Wage Determination AR20260034 dated 2 Jan 2026, provide updates to spec sections 03 30 00, 08 60 45, 08 71 00, 09 06 00, 09 97 13.27, 25 05 11.01, 25 05 11.02, 25 05 11.04, 31 63 26, 41 22 13.15, and EXTEND the proposal due date to 2 FEBRUARY 2026 at 1400 CST. Also delete section 25 05 11.03.

All other terms and conditions remain unchanged. The due date is EXTENDED to 2 FEBRUARY 2026 at 1400 CST. Government POC is Melissa Hyslop via email at melissa.d.hyslop@usace.army.mil.

Except as provided herein, all terms and conditions of the document referenced in Item 9A or 10A, as heretofore changed, remains unchanged and in full force and effect.

15A. NAME AND TITLE OF SIGNER (Type or print)		16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print)	
15B. CONTRACTOR/OFFEROR	15C. DATE SIGNED	16B. UNITED STATES OF AMERICA	16C. DATE SIGNED
(Signature of person authorized to sign)		(Signature of Contracting Officer)	

SECTION SF 30 BLOCK 14 CONTINUATION PAGE SUMMARY OF CHANGES

Section 00 00 00 - Procurement and Contracting Requirements

The following changes have been made:

INFORMATION	FROM	TO
Response Due Date	27 Jan 2026	02 Feb 2026

"General Decision Number: AR20260034 01/02/2026

Superseded General Decision Number: AR20250034

State: Arkansas

Construction Type: Building
BUILDING CONSTRUCTION PROJECTS (does not include single family
homes or apartments up to and including 4 stories).

County: Sebastian County in Arkansas.

Modification Number	Publication Date
0	01/02/2026

BOIL0069-002 01/01/2025

	Rates	Fringes
BOILERMAKER.....	\$ 34.21	23.92

CARP0071-002 01/01/2024

	Rates	Fringes
CARPENTER (Includes Drywall Hanging, and Form Work).....	\$ 31.93	11.83

PAIN0424-008 07/01/2021

	Rates	Fringes
PAINTER (Spray).....	\$ 16.25	10.42

PLUM0155-015 08/01/2025

	Rates	Fringes
PIPEFITTER.....	\$ 34.41	15.70

PLUM0155-017 08/01/2025

	Rates	Fringes
PLUMBER.....	\$ 34.41	15.70

SUAR2015-031 01/09/2017

	Rates	Fringes
BRICKLAYER.....	\$ 19.39	0.00
CEMENT MASON/CONCRETE FINISHER...	\$ 14.79	0.00
ELECTRICIAN.....	\$ 19.91	2.54
INSULATOR - MECHANICAL (Duct, Pipe & Mechanical System Insulation).....	\$ 17.16	4.76
IRONWORKER, REINFORCING.....	\$ 14.00	0.00

IRONWORKER, STRUCTURAL.....	\$ 19.39	0.00
LABORER: Common or General.....	\$ 11.53	0.00
LABORER: Mason Tender - Brick....	\$ 12.04	0.00
LABORER: Pipelayer.....	\$ 14.02	0.00
OPERATOR:		
Backhoe/Excavator/Trackhoe.....	\$ 19.10	0.00
OPERATOR: Bulldozer.....	\$ 16.74	0.00
OPERATOR: Crane.....	\$ 17.52	0.00
OPERATOR: Grader/Blade.....	\$ 14.66	0.00
OPERATOR: Paver (Asphalt, Aggregate, and Concrete).....	\$ 17.79	0.00
OPERATOR: Roller.....	\$ 14.86	2.18
PAINTER (Brush and Roller).....	\$ 13.38	0.00
ROOFER.....	\$ 15.39	0.00
SHEET METAL WORKER, Includes HVAC Duct Installation.....	\$ 20.25	2.73
TRUCK DRIVER: Dump Truck.....	\$ 13.92	0.85

WELDERS - Receive rate prescribed for craft performing operation to which welding is incidental.

=====

Note: Executive Order (EO) 13706, Establishing Paid Sick Leave for Federal Contractors applies to all contracts subject to the Davis-Bacon Act for which the contract is awarded (and any solicitation was issued) on or after January 1, 2017. If this contract is covered by the EO, the contractor must provide employees with 1 hour of paid sick leave for every 30 hours they work, up to 56 hours of paid sick leave each year. Employees must be permitted to use paid sick leave for their own illness, injury or other health-related needs, including preventive care; to assist a family member (or person who is like family to the employee) who is ill, injured, or has other health-related needs, including preventive care; or for reasons resulting from, or to assist a family member (or person who is like family to the employee) who is a victim of, domestic violence, sexual assault, or stalking. Additional information on contractor requirements and worker protections under the EO is available at <https://www.dol.gov/agencies/whd/government-contracts>.

Note: Executive Order 13658 generally applies to contracts subject to the Davis-Bacon Act that were awarded on or between January 1, 2015 and January 29, 2022, and that have not been renewed or extended on or after January 30, 2022. Executive Order 13658 does not apply to contracts subject only to the Davis-Bacon Related Acts regardless of when they were awarded. If a contract is subject to Executive Order 13658, the

contractor must pay all covered workers at least \$13.30 per hour (or the applicable wage rate listed on this wage determination, if it is higher) for all hours spent performing on the contract in 2025. The applicable Executive Order minimum wage rate will be adjusted annually. Additional information on contractor requirements and worker protections under Executive Order 13658 is available at www.dol.gov/whd/govcontracts.

Unlisted classifications needed for work not included within the scope of the classifications listed may be added after award only as provided in the labor standards contract clauses (29CFR 5.5 (a) (1) (iii)).

The body of each wage determination lists the classifications and wage rates that have been found to be prevailing for the type(s) of construction and geographic area covered by the wage determination. The classifications are listed in alphabetical order under rate identifiers indicating whether the particular rate is a union rate (current union negotiated rate), a survey rate, a weighted union average rate, a state adopted rate, or a supplemental classification rate.

Union Rate Identifiers

A four-letter identifier beginning with characters other than "SU", "UAVG", "SA?", or "SC?" denotes that a union rate was prevailing for that classification in the survey. Example: PLUM0198-005 07/01/2024. PLUM is an identifier of the union whose collectively bargained rate prevailed in the survey for this classification, which in this example would be Plumbers. 0198 indicates the local union number or district council number where applicable, i.e., Plumbers Local 0198. The next number, 005 in the example, is an internal number used in processing the wage determination. The date, 07/01/2024 in the example, is the effective date of the most current negotiated rate.

Union prevailing wage rates are updated to reflect all changes over time that are reported to WHD in the rates in the collective bargaining agreement (CBA) governing the classification.

Union Average Rate Identifiers

The UAVG identifier indicates that no single rate prevailed for those classifications, but that 100% of the data reported for the classifications reflected union rates. EXAMPLE: UAVG-OH-0010 01/01/2024. UAVG indicates that the rate is a weighted union average rate. OH indicates the State of Ohio. The next number, 0010 in the example, is an internal number used in producing the wage determination. The date, 01/01/2024 in the example, indicates the date the wage determination was updated to reflect the most current union average rate.

A UAVG rate will be updated once a year, usually in January, to reflect a weighted average of the current rates in the collective bargaining agreements on which the rate is based.

Survey Rate Identifiers

The ""SU"" identifier indicates that either a single non-union rate prevailed (as defined in 29 CFR 1.2) for this classification in the survey or that the rate was derived by computing a weighted average rate based on all the rates reported in the survey for that classification. As a weighted average rate includes all rates reported in the survey, it may include both union and non-union rates. Example: SUFL2022-007 6/27/2024. SU indicates the rate is a single non-union prevailing rate or a weighted average of survey data for that classification. FL indicates the State of Florida. 2022 is the year of the survey on which these classifications and rates are based. The next number, 007 in the example, is an internal number used in producing the wage determination. The date, 6/27/2024 in the example, indicates the survey completion date for the classifications and rates under that identifier.

?SU? wage rates typically remain in effect until a new survey is conducted. However, the Wage and Hour Division (WHD) has the discretion to update such rates under 29 CFR 1.6(c)(1).

State Adopted Rate Identifiers

The ""SA"" identifier indicates that the classifications and prevailing wage rates set by a state (or local) government were adopted under 29 C.F.R 1.3(g)-(h). Example: SAME2023-007 01/03/2024. SA reflects that the rates are state adopted. ME refers to the State of Maine. 2023 is the year during which the state completed the survey on which the listed classifications and rates are based. The next number, 007 in the example, is an internal number used in producing the wage determination. The date, 01/03/2024 in the example, reflects the date on which the classifications and rates under the ?SA? identifier took effect under state law in the state from which the rates were adopted.

WAGE DETERMINATION APPEALS PROCESS

1) Has there been an initial decision in the matter? This can be:

- a) a survey underlying a wage determination
- b) an existing published wage determination
- c) an initial WHD letter setting forth a position on a wage determination matter
- d) an initial conformance (additional classification and rate) determination

On survey related matters, initial contact, including requests for summaries of surveys, should be directed to the WHD Branch of Wage Surveys. Requests can be submitted via email to davisbaconinfo@dol.gov or by mail to:

Branch of Wage Surveys
Wage and Hour Division
U.S. Department of Labor
200 Constitution Avenue, N.W.
Washington, DC 20210

Regarding any other wage determination matter such as conformance decisions, requests for initial decisions should be

directed to the WHD Branch of Construction Wage Determinations. Requests can be submitted via email to BCWD-Office@dol.gov or by mail to:

Branch of Construction Wage Determinations
Wage and Hour Division
U.S. Department of Labor
200 Constitution Avenue, N.W.
Washington, DC 20210

2) If an initial decision has been issued, then any interested party (those affected by the action) that disagrees with the decision can request review and reconsideration from the Wage and Hour Administrator (See 29 CFR Part 1.8 and 29 CFR Part 7). Requests for review and reconsideration can be submitted via email to dba.reconsideration@dol.gov or by mail to:

Wage and Hour Administrator
U.S. Department of Labor
200 Constitution Avenue, N.W.
Washington, DC 20210

The request should be accompanied by a full statement of the interested party's position and any information (wage payment data, project description, area practice material, etc.) that the requestor considers relevant to the issue.

3) If the decision of the Administrator is not favorable, an interested party may appeal directly to the Administrative Review Board (formerly the Wage Appeals Board). Write to:

Administrative Review Board
U.S. Department of Labor
200 Constitution Avenue, N.W.
Washington, DC 20210.

=====

END OF GENERAL DECISION

"

PROJECT TABLE OF CONTENTS

DIVISION 00 - PROCUREMENT AND CONTRACTING REQUIREMENTS

SF 1442	
00 11 00	PRICING SCHEDULE
00 21 00	INSTRUCTIONS, CONDITIONS AND NOTICES TO OFFERORS
00 21 16	INSTRUCTIONS TO PROPOSERS
00 22 00	SUPPLEMENTARY INSTRUCTIONS
00 22 16	GENERAL SUBMISSION REQUIREMENTS, INSTRUCTIONS, EVALUATIONS, AND BASIS OF AWARD
00 45 00	REPRESENTATIONS AND CERTIFICATIONS
00 70 00	CONDITIONS OF THE CONTRACT
00 72 00	GENERAL CONDITIONS
00 73 00	SUPPLEMENTARY CONDITIONS
00 73 46	WAGE DETERMINATIONS

DIVISION 01 - GENERAL REQUIREMENTS

01 00 00.00 44	CONSTRUCTION SCHEDULE
01 00 50	FORMS AND ATTACHMENTS
01 11 00	SUMMARY OF WORK
01 14 00.00 46	WORK RESTRICTIONS (SWL)
01 30 00	ADMINISTRATIVE REQUIREMENTS
01 30 01.00 47	ADDITIONAL ADMINISTRATIVE REQUIREMENTS
01 32 01.00 10	PROJECT SCHEDULE
01 33 00	SUBMITTAL PROCEDURES
01 33 29	SUSTAINABILITY REQUIREMENTS AND REPORTING
01 35 10.00 46	SPECIAL PROJECT PROCEDURES FOR EBBING FIELD
01 35 26	GOVERNMENTAL SAFETY REQUIREMENTS
01 42 00	SOURCES FOR REFERENCE PUBLICATIONS
01 45 00	QUALITY CONTROL
01 45 00.15 10	RESIDENT MANAGEMENT SYSTEM CONTRACTOR MODE (RMS CM)
01 45 35	SPECIAL INSPECTIONS
01 50 00	TEMPORARY CONSTRUCTION FACILITIES AND CONTROLS
01 56 00.00 46	DUST CONTROL
01 57 19	TEMPORARY ENVIRONMENTAL CONTROLS
01 71 23.00 44	SURVEY, LAYOUT, AND OTHER DATA
01 74 19	CONSTRUCTION WASTE MANAGEMENT AND DISPOSAL
01 78 00	CLOSEOUT SUBMITTALS
01 78 23	OPERATION AND MAINTENANCE DATA
01 78 24.00 10	FACILITY DATA REQUIREMENTS
01 91 00.15	BUILDING COMMISSIONING
01 91 00.16	MECHANICAL/BUILDING CONTROL SYSTEMS INTEGRATOR
01 91 19	BUILDING ENCLOSURE COMMISSIONING

DIVISION 02 - EXISTING CONDITIONS

02 41 00	DEMOLITION
----------	------------

DIVISION 03 - CONCRETE

03 30 00	CAST-IN-PLACE CONCRETE
----------	------------------------

DIVISION 04 - MASONRY

04 20 00	UNIT MASONRY
----------	--------------

DIVISION 05 - METALS

05 05 20	POST-INSTALLED CONCRETE AND MASONRY ANCHORS
05 12 00	STRUCTURAL STEEL
05 21 00	STEEL JOIST FRAMING
05 30 00	STEEL DECKS
05 40 00	COLD-FORMED METAL FRAMING
05 50 13	MISCELLANEOUS METAL FABRICATIONS
05 51 33	METAL LADDERS
05 52 00	METAL RAILINGS

DIVISION 06 - WOOD, PLASTICS, AND COMPOSITES

06 10 00	ROUGH CARPENTRY
06 41 16.00 10	PLASTIC-LAMINATE-CLAD ARCHITECTURAL CABINETS
06 61 16	SOLID SURFACING FABRICATIONS

DIVISION 07 - THERMAL AND MOISTURE PROTECTION

07 21 13	BOARD AND BLOCK INSULATION
07 21 16	MINERAL FIBER BLANKET INSULATION
07 22 00	ROOF AND DECK INSULATION
07 27 10	BUILDING AIR BARRIER SYSTEM
07 27 19.01	SELF-ADHERING AIR BARRIERS
07 27 26	FLUID-APPLIED MEMBRANE AIR BARRIERS
07 27 36	SPRAY FOAM AIR BARRIERS
07 42 63	FABRICATED WALL PANEL ASSEMBLIES
07 60 00	FLASHING AND SHEET METAL
07 61 14.00 20	STEEL STANDING SEAM ROOFING
07 84 00	FIRESTOPPING
07 92 00	JOINT SEALANTS

DIVISION 08 - OPENINGS

08 11 13	STEEL DOORS AND FRAMES
08 14 00	WOOD DOORS
08 31 00	ACCESS DOORS AND PANELS
08 33 23	OVERHEAD COILING DOORS
08 34 16.20	VERTICAL LIFT FABRIC DOORS
08 34 73	SOUND CONTROL DOOR ASSEMBLIES
08 41 13	ALUMINUM-FRAMED ENTRANCES AND STOREFRONTS
08 51 13	ALUMINUM WINDOWS
08 60 45	TRANSLUCENT PANELS
08 71 00	DOOR HARDWARE
08 81 00	GLAZING
08 91 00	METAL WALL LOUVERS

DIVISION 09 - FINISHES

09 06 00	SCHEDULES FOR FINISHES
09 22 00	SUPPORTS FOR PLASTER AND GYPSUM BOARD
09 29 00	GYPSUM BOARD
09 30 10	CERAMIC, QUARRY, AND GLASS TILING
09 51 00	ACOUSTICAL CEILINGS
09 67 23.13	STANDARD RESINOUS FLOORING
09 67 23.16	FUEL RESISTIVE RESINOUS FLOORING, 5-COAT SYSTEM
09 90 00	PAINTS AND COATINGS
09 97 13.27	HIGH PERFORMANCE COATING FOR STEEL STRUCTURES

DIVISION 10 - SPECIALTIES

10 14 00.10	EXTERIOR SIGNAGE
10 14 00.20	INTERIOR SIGNAGE
10 21 13	TOILET COMPARTMENTS
10 26 00	WALL AND DOOR PROTECTION
10 28 13	TOILET ACCESSORIES
10 44 16	FIRE EXTINGUISHERS
10 51 13	LOCKERS

DIVISION 11 - EQUIPMENT

11 81 29.00 47	FACILITY FALL PROTECTION
----------------	--------------------------

DIVISION 12 - FURNISHINGS

12 48 13	ENTRANCE FLOOR MATS AND FRAMES
12 50 00.13 10	FURNITURE AND FURNITURE INSTALLATION

DIVISION 21 - FIRE SUPPRESSION

21 13 13	WET PIPE SPRINKLER SYSTEMS, FIRE PROTECTION
21 13 18.00 10	PREACTION SPRINKLER SYSTEMS, FIRE PROTECTION
21 30 00	FIRE PUMPS

DIVISION 22 - PLUMBING

22 00 00	PLUMBING, GENERAL PURPOSE
22 05 48.00 20	MECHANICAL SOUND, VIBRATION, AND SEISMIC CONTROL
22 15 19.19 47	NONLUBRICATED ROTARY SCREW AIR COMPRESSORS

DIVISION 23 - HEATING, VENTILATING, AND AIR CONDITIONING (HVAC)

23 03 00.00 20	BASIC MECHANICAL MATERIALS AND METHODS
23 05 15	COMMON PIPING FOR HVAC
23 05 48.19	BRACING FOR HVAC
23 05 93	TESTING, ADJUSTING, AND BALANCING FOR HVAC
23 07 00	THERMAL INSULATION FOR MECHANICAL SYSTEMS
23 08 00	COMMISSIONING OF MECHANICAL AND PLUMBING SYSTEMS
23 09 00	INSTRUMENTATION AND CONTROL FOR HVAC
23 09 13	INSTRUMENTATION AND CONTROL DEVICES FOR HVAC
23 09 23.02	BACNET DIRECT DIGITAL CONTROL FOR HVAC AND OTHER BUILDING CONTROL SYSTEMS
23 21 13.00 20	LOW TEMPERATURE WATER (LTW) HEATING SYSTEM
23 21 23	HYDRONIC PUMPS
23 23 00	REFRIGERANT PIPING
23 30 00	HVAC AIR DISTRIBUTION
23 52 13.00 47	ELECTRIC BOILERS
23 64 10	WATER CHILLERS, VAPOR COMPRESSION TYPE
23 64 26	CHILLED, CHILLED-HOT, AND CONDENSER WATER PIPING SYSTEMS
23 75 15	CUSTOM-PACKAGED, AIRCRAFT PRE-CONDITIONED AIR UNITS
23 81 00	DECENTRALIZED UNITARY HVAC EQUIPMENT
23 82 00.00 20	TERMINAL HEATING UNITS

DIVISION 25 - INTEGRATED AUTOMATION

25 05 11.01	CYBERSECURITY FOR FACILITY-RELATED CONTROL SYSTEMS: HVAC
-------------	--

	25 05 11.02	CYBERSECURITY FOR FACILITY-RELATED CONTROL SYSTEMS: FIRE ALARM/MASS NOTIFICATION SYSTEM	
AM0003	~~25 05 11.03~~	~~CYBERSECURITY FOR FACILITY-RELATED CONTROL SYSTEMS: ESS~~	AM0003
	25 05 11.04	CYBERSECURITY FOR FACILITY-RELATED CONTROL SYSTEMS: LIGHTING CONTROL SYSTEM	
	25 08 10	UTILITY MONITORING AND CONTROL SYSTEM TESTING	
	25 10 10	UTILITY MONITORING AND CONTROL SYSTEM (UMCS) FRONT END AND INTEGRATION	

DIVISION 26 - ELECTRICAL

	26 05 73	POWER SYSTEM STUDIES
	26 08 00	APPARATUS INSPECTION AND TESTING
	26 20 00	INTERIOR DISTRIBUTION SYSTEM
	26 24 13	SWITCHBOARDS
	26 29 23	ADJUSTABLE SPEED DRIVE (ASD) SYSTEMS UNDER 600 VOLTS
	26 35 44	270 VDC SOLID STATE CONVERTER
	26 41 00	LIGHTNING PROTECTION SYSTEM
	26 42 13	GALVANIC (SACRIFICIAL) ANODE CATHODIC PROTECTION (GACP) SYSTEM
	26 51 00	INTERIOR LIGHTING
	26 56 00	EXTERIOR LIGHTING
	26 56 20	AIRFIELD AND HELIPORT LIGHTING AND VISUAL NAVIGATION AIDS

DIVISION 27 - COMMUNICATIONS

	27 10 00	BUILDING TELECOMMUNICATIONS CABLING SYSTEM
--	----------	--

DIVISION 28 - ELECTRONIC SAFETY AND SECURITY

	28 31 76	INTERIOR FIRE ALARM AND MASS NOTIFICATION SYSTEM, ADDRESSABLE
--	----------	---

DIVISION 31 - EARTHWORK

	31 00 00	EARTHWORK
	31 05 19.13	GEOTEXTILES FOR EARTHWORK
	31 11 00	CLEARING AND GRUBBING
	31 31 16.13	CHEMICAL TERMITE CONTROL
	31 63 26	DRILLED CAISSONS

DIVISION 32 - EXTERIOR IMPROVEMENTS

	32 01 16.71	COLD MILLING ASPHALT PAVING
	32 01 19.61	SEALING OF JOINTS IN RIGID PAVEMENT
	32 11 20	BASE COURSE FOR RIGID AND FOR FLEXIBLE PAVING
	32 11 23	GRADED CRUSHED AGGREGATE BASE COURSE
	32 11 23.23	BASE COURSE DRAINAGE LAYERS
	32 12 13	BITUMINOUS TACK AND PRIME COATS
	32 12 16.16	ROAD-MIX ASPHALT PAVING
	32 13 13.06	PORTLAND CEMENT CONCRETE PAVEMENT FOR ROADS AND SITE FACILITIES
	32 13 14.13	CONCRETE PAVING FOR AIRFIELDS AND OTHER HEAVY DUTY PAVEMENTS
	32 13 73.19	COMPRESSION CONCRETE PAVING JOINT SEALANT
	32 16 19	CONCRETE CURBS, GUTTERS, AND SIDEWALKS
	32 17 23.16	ROAD AND PARKING LOT PAVEMENT MARKINGS
	32 17 23.19	AIRFIELD PAVEMENT MARKINGS

32 31 13.53	HIGH-SECURITY FENCES AND GATES
32 92 19	SEEDING
32 92 23	SODDING

DIVISION 33 - UTILITIES

33 11 00	WATER UTILITY DISTRIBUTION PIPING
33 30 00	SANITARY SEWERAGE AND INDUSTRIAL WASTE PIPING
33 40 00	STORM DRAINAGE UTILITIES
33 46 16	SUBDRAINAGE PIPING
33 56 10	FACTORY-FABRICATED CONTAINMENT TANKS
33 71 02	UNDERGROUND ELECTRICAL DISTRIBUTION
33 82 00	TELECOMMUNICATIONS OUTSIDE PLANT (OSP)

DIVISION 41 - MATERIAL PROCESSING AND HANDLING EQUIPMENT

41 22 13.15	BRIDGE CRANES, OVERHEAD ELECTRIC, UNDER RUNNING TROLLEY
-------------	---

-- End of Project Table of Contents --

SECTION TABLE OF CONTENTS

DIVISION 03 - CONCRETE

SECTION 03 30 00

CAST-IN-PLACE CONCRETE

PART 1 GENERAL

- 1.1 REFERENCES
- 1.2 DEFINITIONS
- *AM0003 1.3 SUBMITTALS AM0003*
- 1.4 MODIFICATION OF REFERENCES
- 1.5 DELIVERY, STORAGE, AND HANDLING
 - 1.5.1 Reinforcement
- 1.6 QUALITY ASSURANCE
 - 1.6.1 Design Data
 - 1.6.1.1 Concrete Mix Design
 - 1.6.2 Shop Drawings
 - 1.6.2.1 Formwork
 - 1.6.2.2 Reinforcing Steel
 - 1.6.3 Control Submittals
 - 1.6.3.1 Concrete Curing Plan
 - 1.6.3.2 Pumping Concrete
 - 1.6.3.3 VOC Content for form release agents, curing compounds, and concrete penetrating sealers
 - 1.6.3.4 Safety Data Sheets
 - 1.6.4 Test Reports
 - 1.6.4.1 Fly Ash and Pozzolan
 - 1.6.4.2 Slag Cement
 - 1.6.4.3 Aggregates
 - 1.6.5 Quality Control Program
 - 1.6.6 Quality Control Personnel Certifications
 - 1.6.6.1 Quality Manager Qualifications
 - 1.6.6.2 Field Testing Technician and Testing Agency
 - 1.6.7 Laboratory Qualifications for Concrete Qualification Testing
 - 1.6.8 Laboratory Accreditation
- 1.7 ENVIRONMENTAL REQUIREMENTS
 - 1.7.1 Submittals for Environmental Performance
- 1.8 SUSTAINABLE DESIGN REQUIREMENTS
 - 1.8.1 Local/Regional Materials
- 1.9 QUALIFICATIONS FOR WELDING WORK

PART 2 PRODUCTS

- 2.1 FORMWORK MATERIALS
 - 2.1.1 Wood Forms
 - 2.1.1.1 Concrete Form Plywood (Standard Rough)
 - 2.1.1.2 Overlaid Concrete Form Plywood (Standard Smooth)
 - 2.1.2 Plastic Forms
 - 2.1.3 Carton Forms
 - 2.1.4 Steel Forms
- 2.2 FORMWORK ACCESSORIES

- 2.2.1 Form Ties
- 2.2.2 Waterstops
 - 2.2.2.1 PVC Waterstop
 - 2.2.2.2 Rubber Waterstop
 - 2.2.2.3 Thermoplastic Elastomeric Rubber Waterstop
 - 2.2.2.4 Hydrophilic Waterstop
- 2.2.3 Biodegradable Form Release Agent
- 2.2.4 Chamfer Materials
- 2.2.5 Construction and movement joints
- 2.2.6 Other Embedded items
- *AM0003 2.2.7 Precast Concrete Retainers AM0003*

2.3 CONCRETE MATERIALS

- 2.3.1 Cementitious Materials
 - 2.3.1.1 Portland Cement
 - 2.3.1.2 Blended Cements
 - 2.3.1.3 Fly Ash
 - 2.3.1.4 Slag Cement
 - 2.3.1.5 Other Supplementary Cementitious Materials
- 2.3.2 Water
- 2.3.3 Aggregate
 - 2.3.3.1 Normal-Weight Aggregate
- 2.3.4 Admixtures

2.4 MISCELLANEOUS MATERIALS

- 2.4.1 Concrete Curing Materials
- 2.4.2 Nonshrink Grout
- 2.4.3 Floor Finish Materials
 - 2.4.3.1 Liquid Chemical Floor Hardeners and Sealers
- 2.4.4 Expansion/Contraction Joint Filler
- 2.4.5 Joint Sealants
 - 2.4.5.1 Horizontal Surfaces, 3 Percent Slope, Maximum
 - 2.4.5.2 Preformed Polychloroprene Elastomeric Type
 - 2.4.5.3 Lubricant for Preformed Compression Seals
- 2.4.6 Vapor Retarder
- 2.4.7 Dovetail Anchor Slot

2.5 CONCRETE MIX DESIGN

- 2.5.1 Properties and Requirements
- 2.5.2 Durability
 - 2.5.2.1 Alkali-Aggregate Reaction
 - 2.5.2.2 Freezing and Thawing Resistance
 - 2.5.2.3 Corrosion and Chloride Content
 - 2.5.2.4 Sulfate Resistance
 - 2.5.2.5 Concrete Temperature
 - 2.5.2.6 Concrete Permeability
- 2.5.3 Trial Mixtures
- 2.5.4 Ready-Mix Concrete

2.6 REINFORCEMENT

- 2.6.1 Reinforcing Bars
 - 2.6.1.1 Bar Mats
 - 2.6.1.2 Headed Shear Stud Reinforcement
- 2.6.2 Mechanical Reinforcing Bar Connectors
- 2.6.3 Wire
- 2.6.4 Welded wire reinforcement
- 2.6.5 Reinforcing Bar Supports
- 2.6.6 Dowels for Load Transfer in Floors
- 2.6.7 Welding

PART 3 EXECUTION

3.1 EXAMINATION

- 3.2 PREPARATION
 - 3.2.1 General
 - 3.2.2 Subgrade Under Slabs on Ground
 - 3.2.3 Edge Forms and Screed Strips for Slabs
 - 3.2.4 Reinforcement and Other Embedded Items
- 3.3 FORMS
 - 3.3.1 Coating
 - 3.3.2 Reuse
 - 3.3.3 Forms for Standard Rough Form Finish
 - 3.3.4 Forms for Standard Smooth Form Finish
 - 3.3.5 Form Ties
 - 3.3.6 Tolerances for Form Construction
 - 3.3.7 Removal of Forms and Supports
 - 3.3.8 Strength of Concrete Required for Removal of Formwork
- 3.4 WATERSTOP INSTALLATION AND SPLICES
 - 3.4.1 PVC Waterstop
 - 3.4.2 Rubber Waterstop
 - 3.4.3 Thermoplastic Elastomeric Rubber Waterstop
 - 3.4.4 Hydrophilic Waterstop
- 3.5 PLACING REINFORCEMENT AND MISCELLANEOUS MATERIALS
 - 3.5.1 General
 - 3.5.2 Vapor Retarder
 - 3.5.3 Reinforcement Supports
 - 3.5.4 Splicing
 - 3.5.5 Future Bonding
 - 3.5.6 Setting Miscellaneous Material
 - 3.5.7 Inspection of Reinforcement
 - 3.5.8 Placing Reinforcement
 - 3.5.9 Spacing of Reinforcing Bars
 - 3.5.10 Concrete Protection for Reinforcement
 - 3.5.11 Welding
- 3.6 BATCHING, MEASURING, MIXING, AND TRANSPORTING CONCRETE
 - 3.6.1 Measuring
 - 3.6.2 Mixing
 - 3.6.3 Transporting
- 3.7 PLACING CONCRETE
 - 3.7.1 Pumping
 - 3.7.2 Cold Weather
 - 3.7.3 Hot Weather
 - 3.7.4 Bonding
- 3.8 WASTE MANAGEMENT
 - 3.8.1 Mixing Equipment
 - 3.8.2 Hardened, Cured Waste Concrete
 - 3.8.3 Reinforcing Steel
 - 3.8.4 Other Waste
- 3.9 SURFACE FINISHES EXCEPT FLOOR, SLAB, AND PAVEMENT FINISHES
 - 3.9.1 Defects
 - 3.9.2 Not Against Forms (Top of Walls)
 - 3.9.3 Formed Surfaces
 - 3.9.3.1 Tolerances
 - 3.9.3.2 As-Cast Rough Form
 - 3.9.3.3 Standard Smooth Finish
- 3.10 FLOOR, SLAB, AND PAVEMENT FINISHES AND MISCELLANEOUS CONSTRUCTION
 - 3.10.1 Finish
 - 3.10.1.1 Scratched
 - 3.10.1.2 Floated
 - 3.10.1.3 Steel Troweled
 - 3.10.1.4 Broomed
 - 3.10.1.5 Pavement

- 3.10.1.6 Chemical-Hardener Treatment
- 3.10.2 Flat Floor Finishes
 - 3.10.2.1 Measurement of Floor Tolerances
 - 3.10.2.2 Remedies for Out of Tolerance Work
- 3.10.3 Concrete Walks
- 3.10.4 Pits and Trenches
- 3.10.5 Curbs and Gutters
- 3.11 JOINTS
 - 3.11.1 Construction Joints
 - 3.11.1.1 Construction Joints for Constructability Purposes
 - 3.11.2 Isolation Joints in Slabs on Ground
 - 3.11.3 Contraction Joints in Slabs on Ground
 - 3.11.4 Sealing Joints in Slabs on Ground
- 3.12 CURING AND PROTECTION
 - 3.12.1 Requirements for Type III, High-Early-Strength Portland Cement
 - 3.12.2 Curing Periods
 - 3.12.3 Curing Formed Surfaces
 - 3.12.4 Curing Unformed Surfaces
 - 3.12.5 Temperature of Concrete During Curing
 - 3.12.6 Protection from Mechanical Injury
 - 3.12.7 Protection After Curing
- 3.13 FIELD QUALITY CONTROL
 - 3.13.1 Aggregate Testing
 - 3.13.1.1 Fine Aggregate
 - 3.13.1.2 Coarse Aggregate
 - 3.13.2 Concrete Sampling
 - 3.13.3 Concrete Testing
 - 3.13.3.1 Slump Tests
 - 3.13.3.2 Temperature Tests
 - 3.13.3.3 Compressive Strength Tests
 - 3.13.3.4 Air Content
 - 3.13.3.5 Strength of Concrete Structure
 - 3.13.3.6 Non-Conforming Materials
 - 3.13.3.7 Testing Concrete Structure for Strength
- 3.14 REPAIR, REHABILITATION AND REMOVAL
 - 3.14.1 Crack Repair
 - 3.14.2 Repair of Weak Surfaces
 - 3.14.3 Failure of Quality Assurance Test Results

-- End of Section Table of Contents --

SECTION 03 30 00
CAST-IN-PLACE CONCRETE

PART 1 GENERAL

1.1 REFERENCES

The publications listed below form a part of this specification to the extent referenced. The publications are referred to within the text by the basic designation only.

AMERICAN CONCRETE INSTITUTE (ACI)

ACI 117	(2010; R 2015) Specifications for Tolerances for Concrete Construction and Materials and Commentary
ACI 121R	(2008) Guide for Concrete Construction Quality Systems in Conformance with ISO 9001
ACI 301	(2020) Specifications for Structural Concrete
ACI 302.1R	(2015) Guide for Concrete Floor and Slab Construction
ACI 304.2R	(2017) Guide to Placing Concrete by Pumping Methods
ACI 304R	(2000; R 2009) Guide for Measuring, Mixing, Transporting, and Placing Concrete
ACI 305R	(2020) Guide to Hot Weather Concreting
ACI 306R	(2016) Guide to Cold Weather Concreting
ACI 308.1	(2023) Specification for Curing Concrete
ACI MNL-2	(2019; 11th Edition) ACI Manual of Concrete Inspection
ACI MNL-15	(2020) Field Reference Manual: Specifications for Concrete Construction ACI 301-20 with Selected ACI References

AMERICAN HARDBOARD ASSOCIATION (AHA)

AHA A135.4	(1995; R 2004) Basic Hardboard
------------	--------------------------------

AMERICAN WELDING SOCIETY (AWS)

AWS D1.4/D1.4M	(2018) Structural Welding Code - Reinforcing Steel
----------------	--

ASTM INTERNATIONAL (ASTM)

ASTM A184/A184M	(2019) Standard Specification for Welded Deformed Steel Bar Mats for Concrete Reinforcement
ASTM A615/A615M	(2022) Standard Specification for Deformed and Plain Carbon-Steel Bars for Concrete Reinforcement

ASTM A706/A706M	(2022a) Standard Specification for Low-Alloy Steel Deformed and Plain Bars for Concrete Reinforcement
ASTM A934/A934M	(2022) Standard Specification for Epoxy-Coated Prefabricated Steel Reinforcing Bars
ASTM A996/A996M	(2016) Standard Specification for Rail-Steel and Axle-Steel Deformed Bars for Concrete Reinforcement
ASTM A1022/A1022M	(2016b) Standard Specification for Deformed and Plain Stainless Steel Wire and Welded Wire for Concrete Reinforcement
ASTM A1044/A1044M	(2016a; Errata 1) Standard Specification for Steel Stud Assemblies for Shear Reinforcement of Concrete
ASTM A1064/A1064M	(2024) Standard Specification for Carbon-Steel Wire and Welded Wire Reinforcement, Plain and Deformed, for Concrete
ASTM C31/C31M	(2024b) Standard Practice for Making and Curing Concrete Test Specimens in the Field
ASTM C33/C33M	(2023) Standard Specification for Concrete Aggregates
ASTM C39/C39M	(2024) Standard Test Method for Compressive Strength of Cylindrical Concrete Specimens
ASTM C42/C42M	(2020) Standard Test Method for Obtaining and Testing Drilled Cores and Sawed Beams of Concrete
ASTM C78/C78M	(2022) Standard Test Method for Flexural Strength of Concrete (Using Simple Beam with Third-Point Loading)
ASTM C94/C94M	(2024d) Standard Specification for Ready-Mixed Concrete
ASTM C136/C136M	(2019) Standard Test Method for Sieve Analysis of Fine and Coarse Aggregates
ASTM C143/C143M	(2020) Standard Test Method for Slump of Hydraulic-Cement Concrete
ASTM C150/C150M	(2022) Standard Specification for Portland Cement
ASTM C157/C157M	(2024; E 2024) Standard Test Method for Length Change of Hardened Hydraulic-Cement Mortar and Concrete
ASTM C172/C172M	(2017) Standard Practice for Sampling Freshly Mixed Concrete
ASTM C173/C173M	(2024) Standard Test Method for Air Content of Freshly Mixed Concrete by the Volumetric Method
ASTM C231/C231M	(2024) Standard Test Method for Air Content of Freshly Mixed Concrete by the Pressure Method
ASTM C260/C260M	(2010a; R 2016) Standard Specification for Air-Entraining Admixtures for Concrete

ASTM C311/C311M	(2024) Standard Test Methods for Sampling and Testing Fly Ash or Natural Pozzolans for Use in Portland-Cement Concrete
ASTM C330/C330M	(2017a) Standard Specification for Lightweight Aggregates for Structural Concrete
ASTM C494/C494M	(2019; E 2022) Standard Specification for Chemical Admixtures for Concrete
ASTM C595/C595M	(2023) Standard Specification for Blended Hydraulic Cements
ASTM C618	(2023; E 2023) Standard Specification for Coal Fly Ash and Raw or Calcined Natural Pozzolan for Use in Concrete
ASTM C803/C803M	(2023) Standard Test Method for Penetration Resistance of Hardened Concrete
ASTM C873/C873M	(2015) Standard Test Method for Compressive Strength of Concrete Cylinders Cast in Place in Cylindrical Molds
ASTM C900	(2015) Standard Test Method for Pullout Strength of Hardened Concrete
ASTM C920	(2018) Standard Specification for Elastomeric Joint Sealants
ASTM C989/C989M	(2024) Standard Specification for Slag Cement for Use in Concrete and Mortars
ASTM C1074	(2019; E 2021) Standard Practice for Estimating Concrete Strength by the Maturity Method
ASTM C1077	(2024) Standard Practice for Agencies Testing Concrete and Concrete Aggregates for Use in Construction and Criteria for Testing Agency Evaluation
ASTM C1107/C1107M	(2020) Standard Specification for Packaged Dry, Hydraulic-Cement Grout (Nonshrink)
ASTM C1157/C1157M	(2023) Standard Performance Specification for Hydraulic Cement
ASTM C1218/C1218M	(2020c) Standard Test Method for Water-Soluble Chloride in Mortar and Concrete
ASTM C1260	(2023) Standard Test Method for Potential Alkali Reactivity of Aggregates (Mortar-Bar Method)
ASTM C1293	(2008; R 2015) Standard Test Method for Determination of Length Change of Concrete Due to Alkali-Silica Reaction
ASTM C1567	(2023) Standard Test Method for Potential Alkali-Silica Reactivity of Combinations of Cementitious Materials and Aggregate (Accelerated Mortar-Bar Method)
ASTM C1602/C1602M	(2022) Standard Specification for Mixing Water Used in Production of Hydraulic Cement Concrete

ASTM C1778	(2023) Standard Guide for Reducing the Risk of Deleterious Alkali-Aggregate Reaction in Concrete
ASTM D412	(2016; R 2021) Standard Test Methods for Vulcanized Rubber and Thermoplastic Elastomers - Tension
ASTM D471	(2016a) Standard Test Method for Rubber Property - Effect of Liquids
ASTM D1751	(2018) Standard Specification for Preformed Expansion Joint Filler for Concrete Paving and Structural Construction (Nonextruding and Resilient Bituminous Types)
ASTM D1752	(2018) Standard Specification for Preformed Sponge Rubber, Cork and Recycled PVC Expansion Joint Fillers for Concrete Paving and Structural Construction
ASTM D2628	(1991; R 2016) Standard Specification for Preformed Polychloroprene Elastomeric Joint Seals for Concrete Pavements
ASTM D2835	(1989; R 2017) Standard Specification for Lubricant for Installation of Preformed Compression Seals in Concrete Pavements
ASTM D5759	(2012; R 2020) Characterization of Coal Fly Ash and Clean Coal Combustion Fly Ash for Potential Uses
ASTM D6690	(2021) Standard Specification for Joint and Crack Sealants, Hot Applied, for Concrete and Asphalt Pavements
ASTM E96/E96M	(2024) Standard Test Methods for Gravimetric Determination of Water Vapor Transmission Rate of Materials
ASTM E329	(2023) Standard Specification for Agencies Engaged in Construction Inspection, Testing, or Special Inspection
ASTM E1155	(2020) Standard Test Method for Determining Floor Flatness and Floor Levelness Numbers
ASTM E1643	(2018a) Standard Practice for Selection, Design, Installation, and Inspection of Water Vapor Retarders Used in Contact with Earth or Granular Fill Under Concrete Slabs
ASTM E1745	(2017; R 2023) Standard Specification for Water Vapor Retarders Used in Contact with Soil or Granular Fill under Concrete Slabs

CONCRETE REINFORCING STEEL INSTITUTE (CRSI)

CRSI 10MSP	(2018; Errata 2019) Manual of Standard Practice
CRSI RB4.1	(2016) Supports for Reinforcement Used in Concrete

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

NIST PS 1

(2009) DOC Voluntary Product Standard PS 1-07,
Structural Plywood

U.S. ARMY CORPS OF ENGINEERS (USACE)

COE CRD-C 104

(1980) Method of Calculation of the Fineness Modulus of
Aggregate

COE CRD-C 513

(1974) Corps of Engineers Specifications for Rubber
Waterstops

COE CRD-C 572

(1974) Corps of Engineers Specifications for
Polyvinylchloride Waterstops

1.2 DEFINITIONS

- a. "Cementitious material" as used herein must include all portland cement, pozzolan, fly ash, and slag cement.
- b. "Exposed to public view" means situated so that it can be seen from eye level from a public location after completion of the building. A public location is accessible to persons not responsible for operation or maintenance of the building.
- c. "Chemical admixtures" are materials in the form of powder or fluids that are added to the concrete to give it certain characteristics not obtainable with plain concrete mixes.
- d. "Supplementary cementing materials" (SCM) include coal fly ash, slag cement, natural or calcined pozzolans, and ultra-fine coal ash when used in such proportions to replace the portland cement that result in improvement to sustainability and durability and reduced cost.
- e. "Design strength" (f'c) is the specified compressive strength of concrete at time(s) specified in this section to meet structural design criteria.
- f. "Mass Concrete" is any concrete system that approaches a maximum temperature of 158 degrees F within the first 72 hours of placement. In addition, it includes all concrete elements with a section thickness of 3 feet or more regardless of temperature.
- g. "Mixture proportioning" is the process of designing concrete mixture proportions to enable it to meet the strength, service life and constructability requirements of the project while minimizing the initial and life-cycle cost.
- h. "Mixture proportions" are the masses or volumes of individual ingredients used to make a unit measure (cubic meter or cubic yard) of concrete.
- i. "Pozzolan" is a siliceous or siliceous and aluminous material, which in itself possesses little or no cementitious value but will, in finely divided form and in the presence of moisture, chemically react with calcium hydroxide at ordinary temperatures to form compounds possessing cementitious properties.
- j. "Workability (or consistence)" is the ability of a fresh (plastic) concrete mix to fill the form/mould properly with the desired work (vibration) and without reducing the concrete's quality. Workability depends on water content, chemical admixtures, aggregate (shape and size distribution), cementitious content and age (level of hydration).

1.3 SUBMITTALS

Government approval is required for submittals with a "G" or "S" classification. Submittals not having

a "G" or "S" classification are for information only. When used, a code following the "G" classification identifies the office that will review the submittal for the Government. Submit the following in accordance with Section 01 33 00 SUBMITTAL PROCEDURES:

SD-01 Preconstruction Submittals

Concrete Curing Plan

Quality Control Program; G

Quality Control Personnel Certifications; G

Quality Control Organizational Chart

Laboratory Accreditation; G Maturity Method Data

SD-02 Shop Drawings

Formwork

Reinforcing Steel; G, DO

SD-03 Product Data

Joint Sealants; G

Joint Filler; G

Formwork Materials

Cementitious Materials; G

Vapor Retarder

Concrete Curing Materials

Reinforcement; G

Liquid Chemical Floor Hardeners and Sealers

Admixtures

Mechanical Reinforcing Bar Connectors

Waterstops

Local/Regional Materials; S

Biodegradable Form Release Agent

Pumping Concrete

Nonshrink Grout

*AM0003 ~~SD-04 Samples~~

~~Slab Finish Sample~~ AM0003*

SD-05 Design Data

Concrete Mix Design; G, DO

SD-06 Test Reports

Concrete Mix Design; G, DO

Fly Ash

Pozzolan

Slag Cement

Aggregates

Tolerance Report Compressive Strength Tests; G, DO
Air Content

Slump Tests

Water

SD-07 Certificates

Reinforcing Bars

Welder Qualifications

VOC Content for Form Release Agents, Curing Compounds, and Concrete Penetrating Sealers

Safety Data Sheets

Field Testing Technician and Testing Agency

SD-08 Manufacturer's Instructions

Liquid Chemical Floor Hardeners and Sealers

Joint Sealants; S

Curing Compound

1.4 MODIFICATION OF REFERENCES

Accomplish work in accordance with ACI publications except as modified herein. Consider the advisory or recommended provisions to be mandatory. Interpret reference to the "Building Official," the "Structural Engineer," and the "Architect/Engineer" to mean the Contracting Officer.

1.5 DELIVERY, STORAGE, AND HANDLING

Follow ACI 301, ACI 304R and ASTM A934/A934M requirements and recommendations. Do not deliver concrete until vapor retarder, forms, reinforcement, embedded items, and chamfer strips are in place and ready for concrete placement. Do not store concrete curing compounds or sealers with materials that have a high capacity to adsorb volatile organic compound (VOC) emissions. Do not store concrete curing compounds or sealers in occupied spaces.

1.5.1 Reinforcement

Store reinforcement of different sizes and shapes in separate piles or racks raised above the ground to avoid excessive rusting. Protect from contaminants such as grease, oil, and dirt. Ensure bar sizes can be accurately identified after bundles are broken and tags removed.

1.6 QUALITY ASSURANCE

1.6.1 Design Data

1.6.1.1 Concrete Mix Design

Sixty days minimum prior to concrete placement, submit a mix design for each strength and type of concrete. Submit all documentation required in [ACI 301](#) Section 4 and as specified in this section. Submit a complete list of materials including type; brand; source and amount of cement, supplementary cementitious materials, and admixtures; and applicable reference specifications. Submit mill test and all other test for cement, supplementary cementitious materials, aggregates, and admixtures. Provide documentation of maximum nominal aggregate size, gradation analysis, percentage retained and passing sieve, and a graph of percentage retained versus sieve size. Provide mix proportion data using at least three different water-cementitious material ratios for each type of mixture, which produce a range of strength encompassing those required for each type of concrete required. If source material changes, resubmit mix proportion data using revised source material. Provide only materials that have been proven by trial mix studies to meet the requirements of this specification, unless otherwise approved in writing by the Contracting Officer. Indicate clearly in the submittal where each mix design is used when more than one mix design is submitted. Resubmit data on concrete components if the qualities or source of components changes. Required average strength can be documented by field experience if field strength test data are available and represent a single group of at least 10 consecutive strength tests for one mixture, using materials and conditions similar to those expected for work, and encompassing a period of not less than 45 days. The average of field strength tests shall equal or exceed f_{cr} . Changes in materials, conditions, and proportions within the test record shall not have been more closely restricted than those for the proposed work. Test records shall not be more than 24 months old. Obtain mix design approval from the contracting officer prior to concrete placement.

1.6.2 Shop Drawings

1.6.2.1 Formwork

Drawings showing details of formwork including, but not limited to; joints, supports, studding and shoring, and sequence of form and shoring removal. Indicate placement schedule, construction, location and method of forming control joints. Include locations of inserts, conduit, sleeves and other embedded items. Reproductions of contract drawings are unacceptable.

Design, fabricate, erect, support, brace, and maintain formwork so that it is able to support, without failure, all vertical and lateral loads that may reasonably be anticipated to be applied to the formwork.

1.6.2.2 Reinforcing Steel

Indicate bending diagrams, assembly diagrams, splicing and laps of bars, shapes, dimensions, and details of bar reinforcing, accessories, and concrete cover. Do not scale dimensions from structural drawings to determine lengths of reinforcing bars. Reproductions of contract drawings are unacceptable.

1.6.3 Control Submittals

1.6.3.1 Concrete Curing Plan

Submit proposed materials, methods and duration for curing concrete elements in accordance with [ACI 308.1](#).

1.6.3.2 Pumping Concrete

Submit proposed materials and methods for pumping concrete. Submittal must include mix designs, pumping equipment including type of pump and size and material for pipe, and maximum length and height concrete is to be pumped.

1.6.3.3 VOC Content for form release agents, curing compounds, and concrete penetrating sealers

Submit certification for the form release agent, curing compounds, and concrete penetrating sealers that indicate the VOC content of each product.

1.6.3.4 Safety Data Sheets

Submit Safety Data Sheets (SDS) for all materials that are regulated for hazardous health effects. SDS must be readily accessible during each work shift to employees when they are at the construction site.

1.6.4 Test Reports

1.6.4.1 Fly Ash and Pozzolan

Submit test results in accordance with **ASTM C618** for fly ash and pozzolan. Submit test results performed within 6 months of submittal date.

1.6.4.2 Slag Cement

Submit test results in accordance with **ASTM C989/C989M** for slag cement. Submit test results performed within 6 months of submittal date.

1.6.4.3 Aggregates

Submit test results in accordance with **ASTM C33/C33M**, or **ASTM C330/C330M** for lightweight aggregate, and **ASTM C1293** or **ASTM C1567** as required in the paragraph titled ALKALI-AGGREGATE REACTION.

1.6.5 Quality Control Program

Develop and submit for approval a concrete quality control program in accordance with the guidelines of **ACI 121R** and as specified herein. The plan must include approved laboratories. Provide direct oversight for the concrete qualification program inclusive of associated sampling and testing. All quality control reports must be provided to the Contracting Officer, Quality Manager and Concrete Supplier. Maintain a copy of **ACI MNL-15** and **CRSI 10MSP** at project site.

1.6.6 Quality Control Personnel Certifications

The Contractor must submit for approval the responsibilities of the various quality control personnel, including the names and qualifications of the individuals in those positions and a **quality control organizational chart** defining the quality control hierarchy and the responsibility of the various positions. Quality control personnel shall have the qualifications listed below or shall have written evidence of having completed similar qualification programs. Quality control personnel must be employed by the Contractor.

Submit American Concrete Institute certification for the following:

- a. CQC personnel responsible for inspection of concrete operations: ACI Concrete Construction Inspector, Level II.
- b. Lead Foreman or Journeyman of the Concrete Placing, Finishing, and Curing Crews.

- c. Field Testing Technicians: ACI Concrete Field Testing Technician, Grade I: ACI Concrete Flatwork Associate of ACI Concrete Flatwork Finisher

1.6.6.1 Quality Manager Qualifications

The quality manager must hold a current license as a professional engineer in a U.S. state or territory with experience on at least five similar projects. Evidence of extraordinary proven experience may be considered by the Contracting Officer as sufficient to act as the Quality Manager.

1.6.6.2 Field Testing Technician and Testing Agency

Submit data on qualifications of proposed testing agency and technicians for approval by the Contracting Officer prior to performing testing on concrete.

- a. Work on concrete under this contract must be performed by an ACI Concrete Field Testing Technician Grade 1 qualified in accordance with [ACI MNL-2](#) or equivalent. Equivalent certification programs must include requirements for written and performance examinations as stipulated in [ACI MNL-2](#).
- b. Testing agencies that perform testing services on reinforcing steel must meet the requirements of [ASTM E329](#).
- c. Testing agencies that perform testing services on concrete materials must meet the requirements of [ASTM C1077](#).

1.6.7 Laboratory Qualifications for Concrete Qualification Testing

The concrete testing laboratory must have the necessary equipment and experience to accomplish required testing. The laboratory must meet the requirements of [ASTM C1077](#) and be Cement and Concrete Reference Laboratory (CCRL) inspected.

1.6.8 Laboratory Accreditation

Laboratory and testing facilities must be provided by and at the expense of the Contractor. The laboratories performing the tests must be accredited in accordance with [ASTM C1077](#), including [ASTM C78/C78M](#) and [ASTM C1260](#). The accreditation must be current and must include the required test methods, as specified. Furthermore, the testing must comply with the following requirements:

- a. Aggregate Testing and Mix Proportioning: Aggregate testing and mixture proportioning studies must be performed by an accredited laboratory and under the direction of a registered professional engineer in a U.S. state or territory competent in concrete materials who is competent in concrete materials and must sign all reports and designs.
- b. Acceptance Testing: Furnish all materials, labor, and facilities required for molding, curing, testing, and protecting test specimens at the site and in the laboratory. Furnish and maintain boxes or other facilities suitable for storing and curing the specimens at the site while in the mold within the temperature range stipulated by [ASTM C31/C31M](#).
- c. Contractor Quality Control: All sampling and testing must be performed by an approved, onsite, independent, accredited laboratory.

1.7 ENVIRONMENTAL REQUIREMENTS

Provide space ventilation according to material manufacturer recommendations, at a minimum, during and following installation of concrete curing compound and sealer. Maintain one of the following ventilation conditions during the curing period or for 72 hours after installation:

- a. Supply 100 percent outside air 24 hours a day.

- b. Supply airflow at a rate of 6 air changes per hour, when outside temperatures are between 55 degrees F and 84 degrees F and humidity is between 30 percent and 60 percent.
- c. Supply airflow at a rate of 1.5 air changes per hour, when outside air conditions are not within the range stipulated above.

1.7.1 Submittals for Environmental Performance

- a. Provide data indication the percentage of post-industrial pozzolan (fly ash, slag cement) cement substitution as a percentage of the full product composite by weight.
- b. Provide data indicating the percentage of post-industrial and post-consumer recycled content aggregate.
- c. Provide product data indicating the percentage of post-consumer recycled steel content in each type of steel reinforcement as a percentage of the full product composite by weight.
- d. Provide product data stating the location where all products were manufactured
- e. For projects using FSC certified formwork, provide chain-of-custody documentation for all certified wood products.
- f. For projects using reusable formwork, provide data showing how formwork is reused.
- g. Provide SDS product information data showing that form release agents meet any environmental performance goals such as using vegetable and soy based products.
- h. Provide SDS product information data showing that concrete adhesives meet any environmental performance goals including low emitting, low volatile organic compound products.

1.8 SUSTAINABLE DESIGN REQUIREMENTS

1.8.1 Local/Regional Materials

Use materials or products extracted, harvested, or recovered, as well as manufactured, within a 500 mile radius from the project site, if available from a minimum of three sources.

1.9 QUALIFICATIONS FOR WELDING WORK

Welding procedures must be in accordance with AWS D1.4/D1.4M.

Verify that Welder qualifications are in accordance with AWS D1.4/D1.4M for welding of reinforcement or under an equivalent qualification test approved in advance. Welders are permitted to do only the type of welding for which each is specifically qualified.

PART 2 PRODUCTS

2.1 FORMWORK MATERIALS

- a. Form-facing material in contact with concrete must be lumber, plywood, tempered concrete-form-grade hardboard, metal, plastic, or treated paper that creates specified appearance and texture of concrete surface. Submit product information on proposed form-facing materials if different from that specified herein.
- b. Design formwork, shores, reshores, and backshores to support loads transmitted to them and to comply with applicable building code requirements.
- c. Design formwork and shoring for load redistribution resulting from stressing of post-tensioned

reinforcement. Ensure that formwork allows movement resulting from application of prestressing force.

- d. Design formwork to withstand pressure resulting from placement and vibration of concrete and to maintain specified tolerances.
- e. Design formwork to accommodate waterstop materials in joints at locations indicated in Contract Documents.
- f. Provide temporary openings in formwork if needed to facilitate cleaning and inspection.
- g. Design formwork joints to inhibit leakage of mortar.
- h. Limit deflection of facing materials for concrete surfaces exposed to view to 1/240 of center-to-center spacing of facing supports.
- i. Do not use earth cuts as forms for vertical or sloping surfaces.
- j. Submit product information on proposed form-facing materials if different from that specified herein.
- k. Submit manufacturer's product data on form liner proposed for use with each formed surface.

2.1.1 Wood Forms

Use lumber as specified in Section 06 10 00 ROUGH CARPENTRY and as follows. Provide lumber that is square edged or tongue-and-groove boards, free of raised grain, knotholes, or other surface defects. Provide plywood that complies with NIST PS 1, B-B concrete form panels or better or AHA A135.4, hardboard for smooth form lining.

2.1.1.1 Concrete Form Plywood (Standard Rough)

Provide plywood that conforms to NIST PS 1, B-B, concrete form, not less than 5/8-inch thick.

2.1.1.2 Overlaid Concrete Form Plywood (Standard Smooth)

Provide plywood that conforms to NIST PS 1, B-B, high density form overlay, not less than 5/8-inch thick.

2.1.2 Plastic Forms

Plastic lumber as specified in Section 06 10 00 ROUGH CARPENTRY. Provide plastic forms that contain a minimum of 50 percent post-consumer recycled content, or a minimum of 50 percent post-industrial recycled content.

2.1.3 Carton Forms

Moisture resistant treated paper faces, biodegradable, structurally sufficient to support weight of wet concrete until initial set. Provide carton forms that contain a minimum of 10 percent post-consumer recycled content, or a minimum of 40 percent post-industrial recycled content.

2.1.4 Steel Forms

Provide steel form surfaces that do not contain irregularities, dents, or sags.

2.2 FORMWORK ACCESSORIES

- a. Use commercially manufactured formwork accessories, including ties and hangers.
- b. Form ties and accessories must not reduce the effective cover of the reinforcement.

2.2.1 Form Ties

- a. Use form ties with ends or end fasteners that can be removed without damage to concrete.
- b. Where indicated in Contract Documents, use form ties with integral water barrier plates or other acceptable positive water barriers in walls.
- c. The breakback distance for ferrous ties must be at least $\frac{3}{4}$ in. for Surface Finish-2.0 or Surface Finish-3.0, as defined in [ACI 301](#).
- d. Submit manufacturer's data sheet on form ties.

2.2.2 Waterstops

Submit manufacturer's data sheet on waterstop materials and splices.

2.2.2.1 PVC Waterstop

Polyvinylchloride waterstops must conform to [COE CRD-C 572](#).

2.2.2.2 Rubber Waterstop

Rubber waterstops must conform to [COE CRD-C 513](#).

2.2.2.3 Thermoplastic Elastomeric Rubber Waterstop

Thermoplastic elastomeric rubber waterstops must conform to [ASTM D471](#).

2.2.2.4 Hydrophilic Waterstop

Swellable strip type compound of polymer modified chloroprene rubber that swells upon contact with water must conform to the following requirements when tested in accordance to [ASTM D412](#): Tensile strength [350 psi](#) minimum; ultimate elongation 600 percent minimum. Hardness must be 50 minimum on the type A durometer and the volumetric expansion ratio in distilled water at [70 degrees F](#) must be 3 to 1 minimum.

2.2.3 Biodegradable Form Release Agent

- a. Provide form release agent that is colorless, biodegradable, and water-based, with a low (maximum of 55 grams/liter (g/l)) VOC content.
- b. Provide product that does not bond with, stain, or adversely affect concrete surfaces and does not impair subsequent treatments of concrete surfaces.
- c. Provide form release agent that reduces formwork moisture absorption, and does not contain diesel fuel, petroleum-based lubricating oils, waxes, or kerosene. Submit documentation indicating type of biobased material in product and biobased content. Indicate relative dollar value of biobased content products to total dollar value of products included in project.
- d. Submit manufacturer's product data on formwork release agent for use on each form-facing material.

2.2.4 Chamfer Materials

Use lumber materials with dimensions of [3/4 x 3/4 in.](#)

2.2.5 Construction and movement joints

- a. Submit details and locations of construction joints in accordance with the requirements herein.
- b. Locate construction joints within middle one-third of spans of slabs, beams, and girders. If a beam intersects a girder within the middle one-third of girder span, the distance between the construction joint in the girder and the edge of the beam must be at least twice the width of the larger member.
- c. Locate construction joints in walls and columns at underside of slabs, beams, or girders and at tops of footings or slabs.
- d. Make construction joints perpendicular to main reinforcement.
- e. Provide movement joints where indicated in Contract Documents or in accepted alternate locations.
- f. Submit location and detail of movement joints if different from those indicated in Contract Documents.
- g. Submit manufacturer's data sheet on expansion joint materials.
- h. Provide keyways where indicated in Contract Documents. Longitudinal keyways indicated in Contract Documents must be at least 1-1/2 in. deep, measured perpendicular to the plane of the joint.

2.2.6 Other Embedded items

Use sleeves, inserts, anchors, and other embedded items of material and design indicated in Contract Documents.

*AM0003 2.2.7 Precast Concrete Retainers

Use ASTM C94/C94M concrete having a minimum compressive strength of 2,500 psi at 28 days.

AM0003*

2.3 CONCRETE MATERIALS

2.3.1 Cementitious Materials

2.3.1.1 Portland Cement

- a. Unless otherwise specified, provide cement that conforms to **ASTM C150/C150M** Type **II**.
- b. Use one brand and type of cement for formed concrete having exposed-to-view finished surfaces.
- c. Submit information along with evidence demonstrating compliance with referenced standards. Submittals must include types of cementitious materials, manufacturing locations, shipping locations, and certificates showing compliance.
- d. Cementitious materials must be stored and kept dry and free from contaminants.

2.3.1.2 Blended Cements

- a. Blended cements must conform to **ASTM C595/C595M** Type IL or **ASTM C1157/C1157M** Type GU. Provide limestone added to the Type IL blend that is interground with cement clinker. Include a written statement from the manufacturer that the amount of limestone in the finished cement does not vary more than plus or minus 2.5 mass percent of the finished cement from lot to lot or within a lot. Limit the percent of slab, pozzolan, or limestone to a maximum of IL(15). The percentage and type of mineral admixture used in the blend is not allowed to change from that submitted for the aggregate evaluation and mixture proportioning.

2.3.1.3 Fly Ash

- a. **ASTM C618**, Class F , except that the maximum allowable loss on ignition must not exceed 3 percent.
- b. If fly ash is used it shall range from 15 to 20 percent by weight of cementitious material, provided the fly ash does not reduce the amount of cement in the concrete mix below the minimum requirements of local building codes. Where the use of fly ash cannot meet the minimum level, it shall not be used. Report the chemical analysis of the fly ash in accordance with **ASTM C311/C311M**. Evaluate and classify fly ash in accordance with **ASTM D5759**.

2.3.1.4 Slag Cement

ASTM C989/C989M, Grade 120.

2.3.1.5 Other Supplementary Cementitious Materials

Natural pozzolan must be raw or calcined and conform to **ASTM C618**, Class N, including the optional requirement for uniformity.

Ultra Fine Fly Ash (UFFA) and Ultra Fine Pozzolan (UFP) must conform to **ASTM C618**, Class F or N, and the following additional requirements:

- a. The strength activity index at 28 days of age must be at least 95 percent of the control specimens.
- b. The average particle size must not exceed 6 microns.
- c. The sum of SiO₂ plus Al₂O₃ plus Fe₂O₃ must be greater than 77 percent.

2.3.2 Water

- a. Water or ice must comply with the requirements of **ASTM C1602/C1602M**.
- b. Minimize the amount of water in the mix. Improve workability by adjusting the grading of the aggregate and using admixture rather than by adding water.
- c. Water must be potable; free from injurious amounts of oils, acids, alkalis, salts, organic materials, or other substances deleterious to concrete.
- d. Protect mixing water and ice from contamination during storage and delivery.
- e. Submit test report showing water complies with **ASTM C1602/C1602M**.

2.3.3 Aggregate

2.3.3.1 Normal-Weight Aggregate

- a. Aggregates must conform to **ASTM C33/C33M**.
- b. Aggregates used in concrete must be obtained from the same sources and have the same size range as aggregates used in concrete represented by submitted field test records or used in trial mixtures.
- c. Store and handle aggregate in a manner that will avoid segregation and prevents contamination by other materials or other sizes of aggregates. Store aggregates in locations that will permit them to drain freely. Do not use aggregates that contain frozen lumps.
- d. Submit types, pit or quarry locations, producers' names, aggregate supplier statement of

compliance with [ASTM C33/C33M](#), and [ASTM C1293](#) expansion data not more than 18 months old.

2.3.4 [Admixtures](#)

- a. Chemical admixtures must conform to [ASTM C494/C494M](#). A high-range water-reducing (HRWR) admixture conforming to [ASTM C494/C494M](#) in concrete mix designs provided that slump does not exceed 8 inches.
- b. Air-entraining admixtures must conform to [ASTM C260/C260M](#) and must be used in concrete mix designs for the exterior surfaces exposed to cold weather.
- c. Do not use calcium chloride admixtures.
- d. Use a corrosion-inhibiting admixture for concrete classified under exposure category C1. Use an ASR-inhibiting admixture for concrete containing aggregate susceptible to ASR.
- e. Admixtures used in concrete must be the same as those used in the concrete represented by submitted field test records or used in trial mixtures.
- f. Protect stored admixtures against contamination, evaporation, or damage.
- g. To ensure uniform distribution of constituents, provide agitating equipment for admixtures used in the form of suspensions or unstable solutions. Protect liquid admixtures from freezing and from temperature changes that would adversely affect their characteristics.
- h. Submit types, brand names, producers' names, manufacturer's technical data sheets, and certificates showing compliance with standards required herein.

2.4 MISCELLANEOUS MATERIALS

2.4.1 [Concrete Curing Materials](#)

Provide concrete curing material in accordance with [ACI 301](#) Section 5 and [ACI 308.1](#) Section 2. Submit product data for concrete [curing compounds](#). Submit manufactures instructions for placement of curing compound.

2.4.2 [Nonshrink Grout](#)

Nonshrink grout in accordance with [ASTM C1107/C1107M](#).

2.4.3 [Floor Finish Materials](#)

2.4.3.1 [Liquid Chemical Floor Hardeners and Sealers](#)

- a. Hardener must be a colorless aqueous solution containing a blend of inorganic silicate or silicate material and proprietary components combined with a wetting agent; that penetrates, hardens, and densifies concrete surfaces. Submit manufactures instructions for placement of liquid chemical floor hardener.
- b. Use concrete penetrating sealers with a low (maximum 100 grams/liter, less water and less exempt compounds) VOC content. Submit manufactures instructions for placement of sealers.

2.4.4 [Expansion/Contraction Joint Filler](#)

[ASTM D1751](#) or [ASTM D1752](#) Type I or Type II. Material must be [1/2 inch](#) thick, unless otherwise indicated.

2.4.5 Joint Sealants

Submit manufacturer's product data, indicating VOC content.

2.4.5.1 Horizontal Surfaces, 3 Percent Slope, Maximum

ASTM D6690 or ASTM C920, Type M, Class 25, Use T.

2.4.5.2 Preformed Polychloroprene Elastomeric Type

ASTM D2628.

2.4.5.3 Lubricant for Preformed Compression Seals

ASTM D2835.

2.4.6 Vapor Retarder

ASTM E1745 Class A polyethylene sheeting, minimum 15 mil thickness or other equivalent material with a maximum permance rating of 0.01 perms per ASTM E96/E96M.

Consider plastic vapor retarders and adhesives with a high recycled content, low toxicity low VOC (Volatile Organic Compounds) levels.

2.4.7 Dovetail Anchor Slot

Preformed metal slot approximately 1 inch by 1 inch of not less than 22 gage galvanized steel cast in concrete. Coordinate actual size and throat opening with dovetail anchors and provide with removable filler material.

2.5 CONCRETE MIX DESIGN

2.5.1 Properties and Requirements

- a. Use materials and material combinations listed in this section and the contract documents.
- b. Cementitious material content must be adequate for concrete to satisfy the specified requirements for strength, w/cm, durability, and finishability described in this section and the contract documents.

The minimum cementitious material content for concrete used in floors must meet the following requirements:

Nominal maximum size of aggregate, in.	Minimum cementitious material content, pounds per cubic yard
1-1/2	470
1	520
3/4	540
3/8	610

- c. Selected target slump must meet the requirements this section, the contract documents, and must not exceed 9 in. Concrete must not show visible signs of segregation.

- d. The target slump must be enforced for the duration of the project. Determine the slump by **ASTM C143/C143M**. Slump tolerances must meet the requirements of **ACI 117**.
- e. Concrete must be air entrained for members assigned to Exposure Class F1, F2, or F3. The total air content must be in accordance with the requirements of the paragraph titled DURABILITY.
- f. Measure air content at the point of delivery in accordance with **ASTM C173/C173M** or **ASTM C231/C231M**.
- g. Concrete for slabs to receive a hard-troweled finish must not contain an air-entraining admixture or have a total air content greater than 3 percent.
- h. Concrete properties and requirements for each portion of the structure are specified in the table below. Refer to the paragraph titled DURABILITY for more details on exposure categories and their requirements.

	Minimum f'_c psi	Exposure Categories [^]	Miscellaneous Requirements
Grade Beams, Drilled Piers and Pier Caps	4500 at 28 days	S0 ; C0 ; W1 ; F2	Max. slump: 6 in. Nominal maximum aggregate size must be 3/4 in.
Slabs-on-grade	4000 at 28 days	S0 ; C0 ; W0 ; F1	Nominal maximum aggregate size must be 3/4 in.
Exterior Slab-on-grade	4500 at 28 days	S0 ; C0 ; W1 ; F2	Nominal maximum aggregate size must be 3/4 in.

2.5.2 Durability

2.5.2.1 Alkali-Aggregate Reaction

Do not use any aggregate susceptible to alkali-carbonate reaction (ACR). Use one of the three

options below for qualifying concrete mixtures to reduce the potential of alkali-silica reaction (ASR):

- a. For each aggregate used in concrete, the expansion result determined in accordance with **ASTM C1293** must not exceed 0.04 percent at one year.
- b. For each aggregate used in concrete, the expansion result of the aggregate and cementitious materials combination determined in accordance with **ASTM C1567** must not exceed 0.10 percent at an age of 16 days.
- c. Alkali content in concrete (LBA) must not exceed **4 pounds per cubic yard** for moderately reactive aggregate or **3 pounds per cubic yard** for highly reactive aggregate. Reactivity must be determined by testing in accordance with **ASTM C1293** and categorized in accordance with **ASTM C1778**. Alkali content is calculated as follows:

$$\text{LBA} = (\text{cement content, pounds per cubic yard}) \times (\text{equivalent alkali content of portland cement in percent}/100 \text{ percent})$$

2.5.2.2 Freezing and Thawing Resistance

- a. Provide concrete meeting the following requirements based on exposure class assigned to members for freezing-and-thawing exposure in Contract Documents:

Exposure class	Maximum <i>w/cm</i> *	Minimum <i>f'c</i> , psi	Air content	Additional Requirements
F0	N/A	2500		N/A
F1	0.55	3500	Depends on aggregate size	N/A
F2	0.45	4500	Depends on aggregate size	See limits on maximum cementitious material by mass

*The maximum *w/cm* limits do not apply to lightweight concrete.

- b. Concrete must be air entrained for members assigned to Exposure Class F1, F2, or F3. The total air content must meet the requirements of the following table:

Nominal maximum aggregate size, in.	Total air content, percent**^	
	Exposure Class F2 and F3	Exposure Class F1
3/8	7.5	6.0
1/2	7.0	5.5
3/4	6.0	5.0
1	6.0	4.5
1-1/2	5.5	4.5

Nominal maximum aggregate size, in.	Total air content, percent ^{*^}	
	Exposure Class F2 and F3	Exposure Class F1
2	5.0	4.0
3	5.5	3.5

*Tolerance on air content as delivered must be plus/minus 1.5 percent.

^For f'c greater than 5000 psi, reducing air content by 1.0 percentage point is acceptable.

- c. Submit documentation verifying compliance with specified requirements.

2.5.2.3 Corrosion and Chloride Content

- a. Provide concrete meeting the requirements of the following table based on the exposure class assigned to members requiring protection against reinforcement corrosion in Contract Documents.
- b. Submit documentation verifying compliance with specified requirements.
- c. Water-soluble chloride ion content contributed from constituents including water, aggregates, cementitious materials, and admixtures must be determined for the concrete mixture by **ASTM C1218/C1218M** at age between 28 and 42 days.
- d. The maximum water-soluble chloride ion (Cl-) content in concrete, percent by mass of cement is as follows:

Exposure class	Maximum w/cm*	Minimum f'c, psi	Maximum water-soluble chloride ion (CL-) content in concrete, percent by mass of cement
Reinforced concrete			
C0	N/A	2500	1.00
C1	N/A	2500	0.30
C2	0.4	5000	0.15

*The maximum w/cm limits do not apply to lightweight concrete.

2.5.2.4 Sulfate Resistance

- a. Provide concrete meeting the requirements of the following table based on the exposure class assigned to members for sulfate exposure.

Exposure class	Maximum w/cm	Minimum f'c, psi	Required cementitious materials-types			Calcium chloride admixture
			ASTM C150/C150M	ASTM C595/C595M	ASTM C1157/C1157M	
S0	N/A	2500	N/A	N/A	N/A	No restrictions

2.5.2.5 Concrete Temperature

The temperature of concrete as delivered must not exceed 95°F .

2.5.2.6 Concrete Permeability

- Provide concrete meeting the requirements of the following table based on exposure class assigned to members requiring low permeability in the Contract Documents.

Exposure class	Maximum w/cm*	Minimum f'c, psi	Additional minimum requirements
W0	N/A	2500	None
W1	0.5	4000	None

*The maximum w/cm limits do not apply to lightweight concrete.

- Submit documentation verifying compliance with specified requirements.

2.5.3 Trial Mixtures

Trial mixtures must be in accordance to ASTM C301.

2.5.4 Ready-Mix Concrete

Provide concrete that meets the requirements of ASTM C94/C94M.

Ready-mixed concrete manufacturer must provide duplicate delivery tickets with each load of concrete delivered. Provide delivery tickets with the following information in addition to that required by ASTM C94/C94M:

- Type and brand cement
- Cement and supplementary cementitious materials content in 94-pound bags per cubic yard of concrete
- Maximum size of aggregate
- Amount and brand name of admixtures
- Total water content expressed by water cementitious material ratio
- Concrete drying shrinkage shall be determined for the approved concrete mixture per ASTM C157/C157M as modified by ACI.

2.6 REINFORCEMENT

Shop Fabricate reinforcing bars to conform to shapes and dimensions indicated for reinforcement, and as follows:

- a. Bend reinforcement cold. Reinforcement must be bent cold to shapes as indicated. Bending must be done in the shop. Rebending of a reinforcing bar that has been bent incorrectly is not permitted. Bending must be in accordance with the standard approved practice and by approved machine methods. Provide hooks and bends that are in accordance with the Contract Documents. Fabricate reinforcement in accordance with fabricating tolerances of [ACI 117](#).
- b. Submit manufacturer's certified test report for reinforcement.
- c. Submit placing drawings showing fabrication dimensions and placement locations of reinforcement and reinforcement supports. Placing drawings must indicate locations of splices, lengths of lap splices, and details of mechanical and welded splices.
- d. Submit request with locations and details of splices not indicated in Contract Documents.
- e. Submit request to place column dowels without using templates.
- f. Submit request for field cutting, including location and type of bar to be cut and reason field cutting is required.

Deliver reinforcing bars bundled, tagged, and marked. Tags must be metal with bar size, length, mark, and other information pressed in by machine. Marks must correspond with those used on the placing drawings.

2.6.1 Reinforcing Bars

- a. Reinforcing bars must be deformed, except spirals, load-transfer dowels, and welded wire reinforcement, which may be plain.
- b. [ASTM A615/A615M](#) with the bars marked S, Grade [60](#); or [ASTM A996/A996M](#) with the bars marked R, Grade [60](#), or marked A, Grade [60](#). See Section [01 33 29 SUSTAINABILITY REQUIREMENTS AND REPORTING](#) for cumulative total recycled content requirements.
- c. Reinforcing bars may contain post-consumer or post-industrial recycled content. Submit documentation indicating percentage of post-industrial and post-consumer recycled content per unit of product. Indicate relative dollar value of recycled content products to total dollar value of products included in project.
- d. Submit mill certificates for reinforcing bars.

2.6.1.1 Bar Mats

- a. Bar mats must conform to [ASTM A184/A184M](#).

2.6.1.2 Headed Shear Stud Reinforcement

Headed studs and headed stud assemblies must conform to [ASTM A1044/A1044M](#).

2.6.2 Mechanical Reinforcing Bar Connectors

- a. Provide 125 percent minimum yield strength of the reinforcement bar.
- b. Submit data on mechanical splices demonstrating compliance with this paragraph.

2.6.3 Wire

- a. Plain or deformed steel wire must conform to [ASTM A1064/A1064M](#).
- b. Stainless steel wire must conform to [ASTM A1022/A1022M](#).

2.6.4 Welded wire reinforcement

- a. Use welded wire reinforcement specified in Contract Documents and conforming to one or more of the specifications given herein.
- b. Plain welded wire reinforcement must conform to [ASTM A1064/A1064M](#), with welded intersections spaced no greater than [12 in.](#) apart in direction of principal reinforcement.
- c. Deformed welded wire reinforcement must conform to [ASTM A1064/A1064M](#), with welded intersections spaced no greater than [16 in.](#) apart in direction of principal reinforcement.

2.6.5 Reinforcing Bar Supports

- a. Provide reinforcement support types within structure as required by Contract Documents. Reinforcement supports must conform to [CRSI RB4.1](#).
- b. Legs of supports in contact with formwork must be hot-dip galvanized, or plastic coated after fabrication, or stainless-steel bar supports.
- c. Minimum 10 percent post-consumer recycled content, or minimum 20 percent post-industrial recycled content. See Section 01 33 29 SUSTAINABILITY REQUIREMENTS AND REPORTING for cumulative total recycled content requirements. Plastic and steel may contain post-consumer or post-industrial recycled content.

2.6.6 Dowels for Load Transfer in Floors

Provide greased dowels for load transfer in floors of the type, design, weight, and dimensions indicated. Provide dowel bars that are plain-billet steel conforming to [ASTM A615/A615M](#), Grade 40.

2.6.7 Welding

- a. Provide weldable reinforcing bars that conform to [ASTM A706/A706M](#) and [ASTM A615/A615M](#) and Supplement S1, Grade [60](#), except that the maximum carbon content must be 0.55 percent.
- b. Comply with [AWS D1.4/D1.4M](#) unless otherwise specified. Do not tack weld reinforcing bars.
- c. Welded assemblies of steel reinforcement produced under factory conditions, such as welded wire reinforcement, bar mats, and deformed bar anchors, are allowed.
- d. After completing welds on zinc-coated (galvanized), epoxy-coated, or zinc and epoxy dual-coated reinforcement, coat welds and repair coating damage as previously specified.

PART 3 EXECUTION

3.1 EXAMINATION

- a. Do not begin installation until substrates have been properly constructed; verify that substrates are level.
- b. If substrate preparation is the responsibility of another installer, notify Contracting Officer of unsatisfactory preparation before processing.

- c. Check field dimensions before beginning installation. If dimensions vary too much from design dimensions for proper installation, notify Contracting Officer and wait for instructions before beginning installation.

3.2 PREPARATION

Contractor to complete a pre-placement conference to discuss project scope and ensure quality control procedures at least 3 days in advance of placing drilled piers, pier caps and grade beams, and slab-on-grade. Determine quantity of concrete needed and minimize the production of excess concrete. Designate locations or uses for potential excess concrete before the concrete is poured.

3.2.1 General

- a. Surfaces against which concrete is to be placed must be free of debris, loose material, standing water, snow, ice, and other deleterious substances before start of concrete placing.
- b. Remove standing water without washing over freshly deposited concrete. Divert flow of water through side drains provided for such purpose.

3.2.2 Subgrade Under Slabs on Ground

- a. Before construction of slabs on ground, have underground work on pipes and conduits completed and approved.
- b. Previously constructed subgrade or fill must be cleaned of foreign materials
- c. Finish surface of capillary water barrier under interior slabs on ground must not show deviation in excess of $\frac{1}{4}$ inch when tested with a 10-foot straightedge parallel with and at right angles to building lines.
- d. Finished surface of subgrade or fill under exterior slabs on ground must not be more than 0.02-foot above or 0.10-foot below elevation indicated.

3.2.3 Edge Forms and Screed Strips for Slabs

- a. Set edge forms or bulkheads and intermediate screed strips for slabs to obtain indicated elevations and contours in finished slab surface and must be strong enough to support vibrating bridge screeds or roller pipe screeds if nature of specified slab finish requires use of such equipment.
- b. Align concrete surface to elevation of screed strips by use of strike-off templates or approved compacting-type screeds.

3.2.4 Reinforcement and Other Embedded Items

- a. Secure reinforcement, joint materials, and other embedded materials in position, inspected, and approved before start of concrete placing.
- b. When concrete is placed, reinforcement must be free of materials deleterious to bond. Reinforcement with rust, mill scale, or a combination of both will be considered satisfactory, provided minimum nominal dimensions, nominal weight, and minimum average height of deformations of a hand-wire-brushed test specimen are not less than applicable ASTM specification requirements.

3.3 FORMS

- a. Provide forms, shoring, and scaffolding for concrete placement. Set forms mortar-tight and true to line and grade.
- b. Chamfer above grade exposed joints, edges, and external corners of concrete 0.75 inch. Place

chamfer strips in corners of formwork to produce beveled edges on permanently exposed surfaces. Do not bevel reentrant corners or edges of formed joints of concrete.

- c. Provide formwork with clean-out openings to permit inspection and removal of debris.
- d. Inspect formwork and remove foreign material before concrete is placed.
- e. At construction joints, lap form-facing materials over the concrete of previous placement. Ensure formwork is placed against hardened concrete so offsets at construction joints conform to specified tolerances.
- f. Provide positive means of adjustment (such as wedges or jacks) of shores and struts. Do not make adjustments in formwork after concrete has reached initial setting. Brace formwork to resist lateral deflection and lateral instability.
- g. Fasten form wedges in place after final adjustment of forms and before concrete placement.
- h. Provide anchoring and bracing to control upward and lateral movement of formwork system.
- i. Construct formwork for openings to facilitate removal and to produce opening dimensions as specified and within tolerances.
- j. Provide runways for moving equipment. Support runways directly on formwork or structural members. Do not support runways on reinforcement. Loading applied by runways must not exceed capacity of formwork or structural members.
- k. Position and support expansion joint materials, waterstops, and other embedded items to prevent displacement. Fill voids in sleeves, inserts, and anchor slots temporarily with removable material to prevent concrete entry into voids.
- l. Clean surfaces of formwork and embedded materials of mortar, grout, and foreign materials before concrete placement.

3.3.1 Coating

- a. Cover formwork surfaces with an acceptable material that inhibits bond with concrete.
- b. If formwork release agent is used, apply to formwork surfaces in accordance with manufacturer's recommendations before placing reinforcement. Remove excess release agent on formwork prior to concrete placement.
- c. Do not allow formwork release agent to contact reinforcement or hardened concrete against which fresh concrete is to be placed.

3.3.2 Reuse

- a. Reuse forms providing the structural integrity of concrete and the aesthetics of exposed concrete are not compromised.
- b. Wood forms must not be clogged with paste and must be capable of absorbing high water-cementitious material ratio paste.
- c. Remove leaked mortar from formwork joints before reuse.

3.3.3 Forms for Standard Rough Form Finish

Provide formwork in accordance with **ACI 301** Section 5 with a surface finish, SF-1.0, for formed surfaces that are to be concealed by other construction.

3.3.4 Forms for Standard Smooth Form Finish

Provide formwork in accordance with **ACI 301** Section 5 with a surface finish, SF-3.0, for formed surfaces that are exposed to view.

3.3.5 Form Ties

- a. After ends or end fasteners of form ties have been removed, repair tie holes in accordance with **ACI 301** Section 5 requirements.

3.3.6 Tolerances for Form Construction

- a. Construct formwork so concrete surfaces conform to tolerances in **ACI 117**.
- b. Position and secure sleeves, inserts, anchors, and other embedded items such that embedded items are positioned within **ACI 117** tolerances.
- c. To maintain specified elevation and thickness within tolerances, install formwork to compensate for deflection and anticipated settlement in formwork during concrete placement. Set formwork and intermediate screed strips for slabs to produce designated elevation, camber, and contour of finished surface before formwork removal. If specified finish requires use of vibrating screeds or roller pipe screeds, ensure that edge forms and screed strips are strong enough to support such equipment.

3.3.7 Removal of Forms and Supports

- a. If vertical formed surfaces require finishing, remove forms as soon as removal operations will not damage concrete.
- b. Remove top forms on sloping surfaces of concrete as soon as removal will not allow concrete to sag. Perform repairs and finishing operations required. If forms are removed before end of specified curing period, provide curing and protection.
- c. Do not damage concrete during removal of vertical formwork for columns, walls, and sides of beams. Perform needed repair and finishing operations required on vertical surfaces. If forms are removed before end of specified curing period, provide curing and protection.
- d. Leave formwork and shoring in place to support construction loads and weight of concrete in beams, slabs, and other structural members until in-place required strength of concrete is reached.
- e. Form-facing material and horizontal facing support members may be removed before in-place concrete reaches specified compressive strength if shores and other supports are designed to allow facing removal without deflection of supported slab or member.

3.3.8 Strength of Concrete Required for Removal of Formwork

If removal of formwork, reshoring, or backshoring is based on concrete reaching a specified in-place strength, mold and field-cure cylinders in accordance with **ASTM C31/C31M**. Test cylinders in accordance with **ASTM C39/C39M**. Alternatively, use one or more of the methods listed herein to evaluate in-place concrete strength for formwork removal.

- a. Tests of cast-in-place cylinders in accordance with **ASTM C873/C873M**. This option is limited to slabs with concrete depths from 5 to 12 in.
- b. Penetration resistance in accordance with **ASTM C803/C803M**.
- c. Pullout strength in accordance with **ASTM C900**.

- d. Maturity method in accordance with [ASTM C1074](#). Submit [maturity method data](#) using project materials and concrete mix proportions used on the project to demonstrate the correlation between maturity and compressive strength of laboratory cured test specimens to the Contracting Officer.

3.4 WATERSTOP INSTALLATION AND SPLICES

- a. Provide waterstops in construction joints as indicated.
- b. Install formwork to accommodate waterstop materials. Locate waterstops in joints where indicated in Contract Documents. Minimize number of splices in waterstop. Splice waterstops in accordance with manufacturer's written instructions. Install factory-manufactured premolded mitered corners.
- c. Install waterstops to form a continuous diaphragm in each joint. Make adequate provisions to support and protect waterstops during progress of work. Protect waterstops protruding from joints from damage.

3.4.1 PVC Waterstop

Make splices by heat sealing the adjacent waterstop edges together using a thermoplastic splicing iron utilizing a non-stick surface specifically designed for waterstop welding. Reform waterstops at splices with a remolding iron with ribs or corrugations to match the pattern of the waterstop. The spliced area, when cooled, must show no signs of separation, holes, or other imperfections when bent by hand in as sharp an angle as possible.

3.4.2 Rubber Waterstop

Rubber waterstops must be spliced using cold bond adhesive as recommended by the manufacturer.

3.4.3 Thermoplastic Elastomeric Rubber Waterstop

Fittings must be shop made using a machine specifically designed to mechanically weld the waterstop. A portable power saw must be used to miter or straight cut the ends to be joined to ensure good alignment and contact between joined surfaces. Maintain continuity of the characteristic features of the cross section of the waterstop (for example ribs, tabular center axis, and protrusions) across the splice.

3.4.4 Hydrophilic Waterstop

Miter cut ends to be joined with sharp knife or shears. The ends must be adhered with adhesive.

3.5 PLACING REINFORCEMENT AND MISCELLANEOUS MATERIALS

- a. Unless otherwise specified, placing reinforcement and miscellaneous materials must be in accordance to [ACI 301](#). Provide bars, welded wire reinforcement, wire ties, supports, and other devices necessary to install and secure reinforcement.
- b. Reinforcement must not have rust, scale, oil, grease, clay, or foreign substances that would reduce the bond. Rusting of reinforcement is a basis of rejection if the effective cross-sectional area or the nominal weight per unit length has been reduced. Remove loose rust prior to placing steel. Tack welding is prohibited.
- c. Nonprestressed cast-in-place concrete members must have concrete cover for reinforcement given in the following table:

Concrete Exposure	Member	Reinforcement	Specified cover, in.
Cast against and permanently in contact with ground	All	All	3
Exposed to weather or in contact with ground	All	No. 6 through No. 18 bars	2
		No. 5 bar, W31 or D31 wire, and smaller	1-1/2
Not exposed to weather or in contact with ground	Slabs, joists, and walls	No. 14 and No. 18 bars	1-1/2
		No. 11 bar and smaller	3/4
	Beams, columns, pedestals, and tension ties	Primary reinforcement, stirrups, ties, spirals, and hoops	1-1/2

3.5.1 General

Provide details of reinforcement that are in accordance with the Contract Documents.

3.5.2 Vapor Retarder

- Install in accordance with **ASTM E1643**. Provide beneath the on-grade concrete floor slab. Use the greatest widths and lengths practicable to eliminate joints wherever possible. Lap joints a minimum of **12 inches** and tape.
- Remove torn, punctured, or damaged vapor retarder material and provide with new vapor retarder prior to placing concrete. Concrete placement must not damage vapor retarder.

3.5.3 Reinforcement Supports

Provide reinforcement support in accordance with **CRSI RB4.1** and **ACI 301** Section 3 requirements. Supports for coated or galvanized bars must also be coated with electrically compatible material for a distance of at least **2 inches** beyond the point of contact with the bars.

3.5.4 Splicing

As indicated in the Contract Documents. For splices not indicated follow **ACI 301**. Do not splice at points of maximum stress. Overlap welded wire reinforcement the spacing of the cross wires, plus **2 inches**.

3.5.5 Future Bonding

Plug exposed, threaded, mechanical reinforcement bar connectors with a greased bolt. Provide bolt threads that match the connector. Countersink the connector in the concrete. Caulk the depression after the bolt is installed.

3.5.6 Setting Miscellaneous Material

Place and secure anchors and bolts, pipe sleeves, conduits, and other such items in position before concrete placement and support against displacement. Plumb anchor bolts and check location and elevation. Temporarily fill voids in sleeves with readily removable material to prevent the entry of concrete.

3.5.7 Inspection of Reinforcement

Inspect and verify proper reinforcement grade, shape, cross section and condition. Do not use reinforcement with the following defects:

- a. Bar lengths, depths, and bends beyond specified fabrication tolerances.
- b. Bends or kinks not indicated on drawings or approved shop drawings.
- c. Bars with reduced cross section due to rusting or other cause.

3.5.8 Placing Reinforcement

Place reinforcement in accordance with [ACI 301](#).

For slabs on grade (over earth or over capillary water barrier), support bars or welded wire reinforcement on precast concrete blocks, spaced at intervals required by size of reinforcement, to keep reinforcement the minimum height specified above the underside of slab or footing.

For slabs other than on grade, supports for which any portion is less than [1 inch](#) from concrete surfaces that are exposed to view or to be painted must be of precast concrete units, plastic-coated steel, or stainless steel protected bar supports. Precast concrete units must be wedge shaped, not larger than [3-1/2 by 3-1/2 inches](#), and of thickness equal to that indicated for concrete protection of reinforcement. Provide precast units that have cast-in galvanized tie wire hooked for anchorage and blend with concrete surfaces after finishing is completed.

Provide reinforcement that is supported and secured together to prevent displacement by construction loads or by placing of wet concrete, and as follows:

- a. Provide supports for reinforcing bars that are sufficient in number and have sufficient strength to carry the reinforcement they support, and in accordance with [ACI 301](#) and [CRSI 10MSP](#). Do not use supports to support runways for concrete conveying equipment and similar construction loads.
- b. Equip supports on ground and similar surfaces with sand-plates.
- c. Support welded wire reinforcement as required for reinforcing bars.
- d. Secure reinforcements to supports by means of tie wire. Wire must be black, soft iron wire, not less than [16 gage](#).
- e. Reinforcement must be accurately placed, securely tied at intersections, and held in position during placing of concrete by spacers, chairs, or other approved supports. Point wire-tie ends away from the form. Unless otherwise indicated, numbers, type, and spacing of supports must conform to the Contract Documents.

- f. Bending of reinforcing bars partially embedded in concrete is permitted only as specified in the Contract Documents.

3.5.9 Spacing of Reinforcing Bars

- a. Spacing must be as indicated in the Contract Documents.
- b. Reinforcing bars may be relocated to avoid interference with other reinforcement, or with conduit, pipe, or other embedded items. If any reinforcing bar is moved a distance exceeding one bar diameter or specified placing tolerance, resulting rearrangement of reinforcement is subject to preapproval by the Contracting Officer.

3.5.10 Concrete Protection for Reinforcement

Additional concrete protection must be in accordance with the Contract Documents.

3.5.11 Welding

Welding must be in accordance with [AWS D1.4/D1.4M](#).

3.6 BATCHING, MEASURING, MIXING, AND TRANSPORTING CONCRETE

In accordance with [ASTM C94/C94M](#), [ACI 301](#), [ACI 302.1R](#) and [ACI 304R](#), except as modified herein. Batching equipment must be such that the concrete ingredients are consistently measured within the following tolerances: 1 percent for cement and water, 2 percent for aggregate, and 3 percent for admixtures. Furnish mandatory batch ticket information for each load of ready mix concrete.

3.6.1 Measuring

Make measurements at intervals as specified in paragraphs SAMPLING and TESTING.

3.6.2 Mixing

- a. Mix concrete in accordance with [ASTM C94/C94M](#), [ACI 301](#) and [ACI 304R](#).
- b. Machine mix concrete. Begin mixing within 30 minutes after the cement has been added to the aggregates. Place concrete within 90 minutes of either addition of mixing water to cement and aggregates or addition of cement to aggregates. A retarder shall be used to facilitate placing and finishing when concrete temperature is [85 degrees F](#) or greater.
- c. If the entrained air content falls below the specified limit, add a sufficient quantity of admixture, within the manufacturer's recommended dosage, to bring the entrained air content within the specified limits. Dissolve admixtures in the mixing water and mix in the drum to uniformly distribute the admixture throughout the batch. Do not reconstitute concrete that has begun to solidify.
- d. When fibers are used, add fibers together with the aggregates and never as the first component in the mixer. Fibers must be dispensed into the mixing system using appropriate dispensing equipment and procedure as recommended by the manufacturer.

3.6.3 Transporting

Transport concrete from the mixer to the forms as rapidly as practicable. Prevent segregation or loss of ingredients. Clean transporting equipment thoroughly before each batch. Do not use aluminum pipe or chutes. Remove concrete which has segregated in transporting and dispose of as directed.

3.7 PLACING CONCRETE

Place concrete in accordance with [ACI 301](#) Section 5. Concrete shall be placed within 15 minutes of

discharge into non-agitating equipment.

3.7.1 Pumping

ACI 304R and **ACI 304.2R**. Pumping must not result in separation or loss of materials nor cause interruptions sufficient to permit loss of plasticity between successive increments. Loss of slump in pumping equipment must not exceed **2 inches** at discharge/placement. Do not convey concrete through pipe made of aluminum or aluminum alloy. Avoid rapid changes in pipe sizes. Limit maximum size of course aggregate to 33 percent of the diameter of the pipe. Limit maximum size of well-rounded aggregate to 40 percent of the pipe diameter. Take samples for testing at both the point of delivery to the pump and at the discharge end.

3.7.2 Cold Weather

Cold weather concrete must meet the requirements of **ACI 301** unless otherwise specified. Do not allow concrete temperature to decrease below **50 degrees F**. Obtain approval prior to placing concrete when the ambient temperature is below **40 degrees F** or when concrete is likely to be subjected to freezing temperatures within 24 hours. Cover concrete and provide sufficient heat to maintain **50 degrees F** minimum adjacent to both the formwork and the structure while curing. Limit the rate of cooling to **5 degrees F** in any one hour and **18 degrees F** per 24 hours after heat application.

3.7.3 Hot Weather

Hot weather concrete must meet the requirements of **ACI 301** unless otherwise specified. Maintain required concrete temperature using Figure 4.2 in **ACI 305R** to prevent the evaporation rate from exceeding **0.2 pound of water per square foot** of exposed concrete per hour. Cool ingredients before mixing or use other suitable means to control concrete temperature and prevent rapid drying of newly placed concrete. Shade the fresh concrete as soon as possible after placing. Start curing when the surface of the fresh concrete is sufficiently hard to permit curing without damage. Provide water hoses, pipes, spraying equipment, and water hauling equipment, where job site is remote to water source, to maintain a moist concrete surface throughout the curing period. Provide burlap cover or other suitable, permeable material with fog spray or continuous wetting of the concrete when weather conditions prevent the use of either liquid membrane curing compound or impervious sheets. For vertical surfaces, protect forms from direct sunlight and add water to top of structure once concrete is set.

3.7.4 Bonding

Surfaces of set concrete at joints, must be roughened and cleaned of laitance, coatings, loose particles, and foreign matter. Roughen surfaces in a manner that exposes the aggregate uniformly and does not leave laitance, loosened particles of aggregate, nor damaged concrete at the surface.

Obtain bonding of fresh concrete that has set as follows:

- a. At joints between footings and walls or columns, between walls or columns and the beams or slabs they support, and elsewhere unless otherwise specified; roughened and cleaned surface of set concrete must be dampened, but not saturated, immediately prior to placing of fresh concrete.
- b. At joints in exposed-to-view work; at vertical joints in walls; at joints near midpoint of span in girders, beams, supported slabs, other structural members; in work designed to contain liquids; the roughened and cleaned surface of set concrete must be dampened but not saturated and covered with a cement grout coating.
- c. Provide cement grout that consists of equal parts of portland cement and fine aggregate by weight with not more than **6 gallons** of water per sack of cement. Apply cement grout with a stiff broom or brush to a minimum thickness of **1/16 inch**. Deposit fresh concrete before cement grout has attained its initial set.

3.8 WASTE MANAGEMENT

Provide as specified in the Waste Management Plan and as follows.

3.8.1 Mixing Equipment

Before concrete pours, designate on-site area to be paved later in project for cleaning out concrete mixing trucks. Minimize water used to wash equipment.

3.8.2 Hardened, Cured Waste Concrete

Use hardened, cured waste concrete as aggregate in concrete mix if approved by Contracting Officer.

3.8.3 Reinforcing Steel

Collect reinforcing steel and place in designated area for recycling.

3.8.4 Other Waste

Identify concrete manufacturer's or supplier's policy for collection or return of construction waste, unused material, deconstruction waste, and/or packaging material. Institute deconstruction and construction waste separation and recycling for use in manufacturer's programs. When such a program is not available, seek local recyclers to reclaim the materials.

3.9 SURFACE FINISHES EXCEPT FLOOR, SLAB, AND PAVEMENT FINISHES

3.9.1 Defects

Repair surface defects in accordance with [ACI 301](#) Section 5.

3.9.2 Not Against Forms (Top of Walls)

Surfaces not otherwise specified must be finished with wood floats to even surfaces. Finish must match adjacent finishes.

3.9.3 Formed Surfaces

3.9.3.1 Tolerances

Tolerances in accordance with [ACI 117](#) and as indicated.

3.9.3.2 As-Cast Rough Form

Provide for surfaces not exposed to public view a surface finish SF-1.0. Patch holes and defects in accordance with [ACI 301](#).

3.9.3.3 Standard Smooth Finish

Provide for surfaces exposed to public view a surface finish SF-3.0. Patch holes and defects in accordance with [ACI 301](#).

3.10 FLOOR, SLAB, AND PAVEMENT FINISHES AND MISCELLANEOUS CONSTRUCTION

In accordance with [ACI 301](#) and [ACI 302.1R](#), unless otherwise specified. Slope floors uniformly to drains where drains are provided. Depress the concrete base slab where quarry tile, ceramic tile, or walk-off mats are indicated. Where straightedge measurements are specified, Contractor must provide straightedge.

3.10.1 Finish

Place, consolidate, and immediately strike off concrete to obtain proper contour, grade, and elevation before bleedwater appears. Permit concrete to attain a set sufficient for floating and supporting the weight of the finisher and equipment. If bleedwater is present prior to floating the surface, drag the excess water off or remove by absorption with porous materials. Do not use dry cement to absorb bleedwater. Grate tampers ("jitterbugs") shall not be used.

3.10.1.1 Scratched

Use for surfaces intended to receive bonded applied cementitious applications. Finish concrete in accordance with **ACI 301** Section 5 for a scratched finish.

3.10.1.2 Floated

Use for exterior slabs where not otherwise specified. Finish concrete in accordance with **ACI 301** Section 5 for a floated finish.

3.10.1.3 Steel Troweled

Use for floors intended as walking surfaces, and for reception of floor coverings. Finish concrete in accordance with **ACI 301** Section 5 for a steel troweled finish.

3.10.1.4 Broomed

Use on surfaces of exterior walks, platforms, patios, and ramps, unless otherwise indicated. Finish concrete in accordance with **ACI 301** Section 5 for a broomed finish.

3.10.1.5 Pavement

Screed the concrete with a template advanced with a combined longitudinal and crosswise motion. Maintain a slight surplus of concrete ahead of the template. After screeding, float the concrete longitudinally. Use a straightedge to check slope and flatness; correct and refloat as necessary. Obtain final finish by a burlap drag. Drag a strip of clean, wet burlap from **3 to 10 feet wide and 2 feet longer** than the pavement width across the slab. Produce a fine, granular, sandy textured surface without disfiguring marks. Round edges and joints with an edger having a radius of **1/8 inch**.

3.10.1.6 Chemical-Hardener Treatment

Apply liquid-chemical floor hardener where indicated after curing and drying concrete surface. Dilute liquid hardener with water and apply in three coats. First coat must be one-third strength, second coat one-half strength, and third coat two-thirds strength. Apply each coat evenly and allow to dry 24 hours between coats.

Approved proprietary chemical hardeners must be applied in accordance with manufacturer's printed directions.

3.10.2 Flat Floor Finishes

ACI 302.1R. Construct in accordance with one of the methods recommended in Table 10.15.3a, "Slab-on-ground flatness/levelness construction guide" or Table 10.15.3b, "Suspended slab flatness/levelness construction guide" appropriate for the type of construction. **ACI 117** for tolerance tested by **ASTM E1155**.

a. Specified Conventional Value:

Floor Flatness (Ff) 25, 20 minimum

3.10.2.1 Measurement of Floor Tolerances

Test slab within 24 hours of the final troweling. Provide tests to Contracting Officer within 12 hours after collecting the data. Floor flatness inspector is required to provide a [tolerance report](#) which must include:

- a. Key plan showing location of data collected.
- b. Results required by [ASTM E1155](#).

3.10.2.2 Remedies for Out of Tolerance Work

Contractor is required to repair and retest any floors not meeting specified tolerances. Prior to repair, Contractor must submit and receive approval for the proposed repair, including product data from any materials proposed. Repairs must not result in damage to structural integrity of the floor. For floors exposed to public view, repairs must prevent any uneven or unusual coloring of the surface.

3.10.3 Concrete Walks

Provide [4 inches](#) thick minimum. Provide contraction joints spaced every [5 linear feet](#) unless otherwise indicated. Cut contraction joints [1 inch](#) deep, or one fourth the slab thickness whichever is deeper, with a jointing tool after the surface has been finished. Provide [0.5 inch](#) thick transverse expansion joints at changes in direction where sidewalk abuts curb, steps, rigid pavement, or other similar structures; space expansion joints every [50 feet](#) maximum. Give walks a broomed finish. Unless indicated otherwise, provide a transverse slope of 1/48. Limit variation in cross section to [1/4 inch in 5 feet](#).

3.10.4 Pits and Trenches

Place bottoms and walls monolithically or provide waterstops and keys.

3.10.5 Curbs and Gutters

Provide contraction joints spaced every [10 feet](#) maximum unless otherwise indicated. Cut contraction joints [3/4 inch](#) deep with a jointing tool after the surface has been finished. Provide expansion joints [1/2 inch](#) thick and spaced every [100 feet](#) maximum unless otherwise indicated. Perform pavement finish.

3.11 JOINTS

3.11.1 Construction Joints

Make and locate joints not indicated so as not to impair strength and appearance of the structure, as approved. Joints must be perpendicular to main reinforcement. Reinforcement must be continued and developed across construction joints. Locate construction joints as follows:

3.11.1.1 Construction Joints for Constructability Purposes

- a. In walls, at top of footing; at top of slabs on ground; at top and bottom of door and window openings or where required to conform to architectural details; and at underside of deepest beam or girder framing into wall.
- b. In columns or piers, at top of footing; at top of slabs on ground; and at underside of deepest beam or girder framing into column or pier.
- c. Near midpoint of spans for supported slabs, beams, and girders unless a beam intersects a girder at the center, in which case construction joints in girder must offset a distance equal to twice the width of the beam. Make transfer of shear through construction joint by use of inclined reinforcement.

Provide keyways at least 1-1/2-inches deep in construction joints in walls and between walls and footings.

3.11.2 Isolation Joints in Slabs on Ground

- a. Provide joints at points of contact between slabs on ground and vertical surfaces, such as column pedestals, foundation walls, grade beams, and elsewhere as indicated.
- b. Fill joints with premolded joint filler strips 1/2 inch thick, extending full slab depth. Install filler strips at proper level below finish floor elevation with a slightly tapered, dress-and-oiled wood strip temporarily secured to top of filler strip to form a groove not less than 3/4 inch in depth where joint is sealed with sealing compound and not less than 1/4 inch in depth where joint sealing is not required. Remove wood strip after concrete has set. Contractor must clean groove of foreign matter and loose particles after surface has dried.

3.11.3 Contraction Joints in Slabs on Ground

- a. Provide joints to form panels as indicated.
- b. Sawcut contraction joints into slab on ground in accordance with ACI 301 Section 5.

3.11.4 Sealing Joints in Slabs on Ground

- a. Contraction and control joints which are to receive finish flooring material must be sealed with joint sealing compound after concrete curing period. Slightly underfill groove with joint sealing compound to prevent extrusion of compound. Remove excess material as soon after sealing as possible.
- b. Sealed groove must be left ready to receive filling material that is provided as part of finish floor covering work.

3.12 CURING AND PROTECTION

Curing and protection in accordance with ACI 301 Section 5, unless otherwise specified. Begin curing immediately following form removal. Avoid damage to concrete from vibration created by blasting, pile driving, movement of equipment in the vicinity, disturbance of formwork or protruding reinforcement, and any other activity resulting in ground vibrations. Protect concrete from injurious action by sun, rain, flowing water, frost, mechanical injury, tire marks, and oil stains. Do not allow concrete to dry out from time of placement until the expiration of the specified curing period. Do not use membrane-forming compound on surfaces where appearance would be objectionable, on any surface to be painted, where coverings are to be bonded to the concrete, or on concrete to which other concrete is to be bonded. If forms are removed prior to the expiration of the curing period, provide another curing procedure specified herein for the remaining portion of the curing period. Provide moist curing for those areas receiving liquid chemical sealer, hardener, or epoxy coating. Allow curing compound/sealer installations to cure prior to the installation of materials that adsorb VOCs, including .

3.12.1 Requirements for Type III, High-Early-Strength Portland Cement

The curing periods are required to be not less than one-fourth of those specified for portland cement, but in no case less than 72 hours.

3.12.2 Curing Periods

ACI 301 Section 5, except 10 days for retaining walls, pavement or chimneys. Begin curing immediately after placement. Protect concrete from premature drying, excessively hot temperatures, and mechanical injury; and maintain minimal moisture loss at a relatively constant temperature for the period necessary for hydration of the cement and hardening of the concrete. The materials and methods of curing are subject to approval by the Contracting Officer.

3.12.3 Curing Formed Surfaces

Accomplish curing of formed surfaces, including undersurfaces of girders, beams, supported slabs, and other similar surfaces by moist curing with forms in place for full curing period or until forms are removed. If forms are removed before end of curing period, accomplish final curing of formed surfaces by any of the curing methods specified above, as applicable.

3.12.4 Curing Unformed Surfaces

- a. Accomplish initial curing of unformed surfaces, such as monolithic slabs, floor topping, and other flat surfaces, by membrane curing.
- b. Accomplish final curing of unformed surfaces by any of curing methods specified, as applicable.
- c. Accomplish final curing of concrete surfaces to receive liquid floor hardener or finish flooring by moisture-retaining cover curing.

3.12.5 Temperature of Concrete During Curing

When temperature of atmosphere is 41 degrees F and below, maintain temperature of concrete at not less than 55 degrees F throughout concrete curing period or 45 degrees F when the curing period is measured by maturity. When necessary, make arrangements before start of concrete placing for heating, covering, insulation, or housing as required to maintain specified temperature and moisture conditions for concrete during curing period.

When the temperature of atmosphere is 80 degrees F and above or during other climatic conditions which cause too rapid drying of concrete, make arrangements before start of concrete placing for installation of wind breaks, of shading, and for fog spraying, wet sprinkling, or moisture-retaining covering of light color as required to protect concrete during curing period.

Changes in temperature of concrete must be uniform and not exceed 5 degrees F in any one hour nor 49 degrees F in any 24-hour period.

3.12.6 Protection from Mechanical Injury

During curing period, protect concrete from damaging mechanical disturbances, particularly load stresses, heavy shock, and excessive vibration and from damage caused by rain or running water.

3.12.7 Protection After Curing

Protect finished concrete surfaces from damage by construction operations.

3.13 FIELD QUALITY CONTROL

3.13.1 Aggregate Testing

3.13.1.1 Fine Aggregate

At least once during each shift when the concrete plant is operating, there shall be one sieve analysis and fineness modulus determination in accordance with ASTM C136/C136M and COE CRD-C 104 for the fine aggregate or for each fine aggregate if it is batched in more than one size or classification. The location at which samples are taken may be selected by the Contractor as the most advantageous for control. However, the Contractor is responsible for delivering fine aggregate to the mixer within specification limits. When the amount passing on any sieve is outside the specification limits, the fine aggregate shall be immediately resampled and retested. If there is another failure on any sieve, the fact shall be immediately reported to the Contracting Officer, concreting shall be stopped, and immediate steps taken to correct the grading.

3.13.1.2 Coarse Aggregate

At least once during each shift in which the concrete plant is operating, there shall be a sieve analysis in accordance with **ASTM C136/C136M** for each size of coarse aggregate. The location at which samples are taken may be selected by the Contractor as the most advantageous for production control. However, the Contractor shall be responsible for delivering the aggregate to the mixer within specification limits. A test record of samples of aggregate taken at the same locations shall show the results of the current test as well as the average results of the five most recent tests including the current test. The Contractor may adopt limits for control coarser than the specification limits for samples taken other than as delivered to the mixer to allow for degradation during handling. When the amount passing any sieve is outside the specification limits, the coarse aggregate shall be immediately resampled and retested. If the second sample fails on any sieve, that fact shall be reported to the Contracting Officer. Where two consecutive averages of 5 tests are outside specification limits, the operation shall be considered out of control and reported to the Contracting Officer. Concreting shall be stopped and immediate steps shall be taken to correct the grading.

3.13.2 Concrete Sampling

ASTM C172/C172M. Collect samples of fresh concrete to perform tests specified. **ASTM C31/C31M** for making test specimens.

3.13.3 Concrete Testing

3.13.3.1 Slump Tests

ASTM C143/C143M. Take concrete samples during concrete placement/discharge. The maximum slump may be increased as specified with the addition of an approved admixture provided that the water-cementitious material ratio is not exceeded. Perform tests at commencement of concrete placement, when test cylinders are made, and for each 20 cubic yards (maximum) of concrete.

3.13.3.2 Temperature Tests

Test the concrete delivered and the concrete in the forms. Perform tests in hot or cold weather conditions (**below 50 degrees F and above 80 degrees F**) for each batch (minimum) or every **20 cubic yards** (maximum) of concrete, until the specified temperature is obtained, and whenever test cylinders and slump tests are made.

3.13.3.3 Compressive Strength Tests

ASTM C39/C39M. Make eight **6 inch by 12 inch** or twelve **4 inch by 8 inch** test cylinders for each set of tests in accordance with **ASTM C31/C31M**, **ASTM C172/C172M** and applicable requirements of **ACI 305R** and **ACI 306R**. Take precautions to prevent evaporation and loss of water from the specimen. Test two **6 inch by 12 inch** or three **4 inch by 8 inch** cylinders at 7 days, two **6 inch by 12 inch** or three **4 inch by 8 inch** cylinders at 28 days, and hold four **6 inch by 12 inch** or six **4 inch by 8 inch** cylinders in reserve. Take samples for strength tests for each concrete mixture placed each day not less than once a day, nor less than once for each **150 cubic yards** of concrete, nor less than once for each **5000 square feet** of surface area for slabs or walls. For the entire project, take no less than five sets of samples and perform strength tests for each mix design of concrete placed. Each strength test result must be the average of two **6 inch by 12 inch** or three **4 inch by 8 inch** cylinders from the same concrete sample tested at 28 days. Concrete compressive tests must meet the requirements of this section, the Contract Document, and **ACI 301**.

3.13.3.4 Air Content

ASTM C173/C173M or **ASTM C231/C231M** for normal weight concrete. Test air-entrained concrete for air content at the same frequency as specified for slump tests.

3.13.3.5 Strength of Concrete Structure

The strength of the concrete structure will be considered to be deficient if any of the following conditions are identified:

- a. Failure to meet compressive strength tests as evaluated.
- b. Reinforcement not conforming to requirements specified.
- c. Concrete which differs from required dimensions or location in such a manner as to reduce strength.
- d. Concrete curing and protection of concrete against extremes of temperature during curing, not conforming to requirements specified.
- e. Concrete subjected to damaging mechanical disturbances, particularly load stresses, heavy shock, and excessive vibration.
- f. Poor workmanship likely to result in deficient strength.

Where the strength of the concrete structure is considered deficient submit a mitigation or remediation plan for review and approval by the contracting officer.

3.13.3.6 Non-Conforming Materials

Factors that indicate that there are non-conforming materials include (but not limited to) excessive compressive strength, inadequate compressive strength, excessive slump, excessive voids and honeycombing, concrete delivery records that indicate excessive time between mixing and placement, or excessive water was added to the mixture during delivery and placement. Any of these indicators alone are sufficient reason for the Contracting Officer to request additional sampling and testing.

Investigations into non-conforming materials must be conducted at the Contractor's expense. The Contractor must be responsible for the investigation and must make written recommendations to adequately mitigate or remediate the non-conforming material. The Contracting Officer may accept, accept with reduced payment, require mitigation, or require removal and replacement of non-conforming material at no additional cost to the Government.

3.13.3.7 Testing Concrete Structure for Strength

When there is evidence that strength of concrete structure in place does not meet specification requirements or there are non-conforming materials, make cores drilled from hardened concrete for compressive strength determination in accordance with [ASTM C42/C42M](#), and as follows:

- a. Take at least three representative cores from each member or area of concrete-in-place that is considered potentially deficient. Location of cores will be determined by the Contracting Officer.
- b. Test cores after moisture conditioning in accordance with [ASTM C42/C42M](#) if concrete they represent is more than superficially wet under service.
- c. Air dry cores, ([60 to 80 degrees F](#) with relative humidity less than 60 percent) for 7 days before test and test dry if concrete they represent is dry under service conditions.
- d. Strength of cores from each member or area are considered satisfactory if their average compressive strength is equal to or greater than 85 percent of the design compressive strength, and if no single core strength is less than 75 percent of the design compressive strength. Additional testing of cores extracted from locations represented by erratic core strength results will be permitted only when approved by the Contracting Officer.

Fill core holes solid with patching mortar and finished to match adjacent concrete surfaces.

Correct concrete work that is found inadequate by core tests in a manner approved by the Contracting Officer.

3.14 REPAIR, REHABILITATION AND REMOVAL

Before the Contracting Officer accepts the structure the Contractor must inspect the structure for cracks, damage and substandard concrete placements that may adversely affect the service life of the structure. A report documenting these defects must be prepared which includes recommendations for repair, removal or remediation must be submitted to the Contracting Officer for approval before any corrective work is accomplished.

3.14.1 Crack Repair

Prior to final acceptance, all cracks in excess of 0.02 inches wide must be documented and repaired. The proposed method and materials to repair the cracks must be submitted to the Contracting Officer for approval. The proposal must address the amount of movement expected in the crack due to temperature changes and loading.

3.14.2 Repair of Weak Surfaces

Weak surfaces are defined as mortar-rich, rain-damaged, uncured, or containing exposed voids or deleterious materials. Concrete surfaces with weak surfaces less than 1/4 inch thick must be diamond ground to remove the weak surface. Surfaces containing weak surfaces greater than 1/4 inch thick must be removed and replaced or mitigated in a manner acceptable to the Contracting Officer.

3.14.3 Failure of Quality Assurance Test Results

Proposed mitigation efforts by the Contractor must be approved by the Contracting Officer prior to proceeding.

-- End of Section --

SECTION TABLE OF CONTENTS

DIVISION 08 - OPENINGS

SECTION 08 60 45

TRANSLUCENT PANELS

PART 1 GENERAL

- 1.1 SUMMARY
- 1.2 REFERENCES
- 1.3 SUBMITTALS
- 1.4 QUALITY ASSURANCE
- 1.5 DELIVERY, STORAGE, AND HANDLING
- 1.6 WARRANTY

PART 2 PRODUCTS

- 2.1 TRANSLUCENT PANELS
- 2.2 GLASS-FIBER PANELS
 - 2.2.1 Weatherability
 - 2.2.2 Non Combustible Grid Core
 - 2.2.3 Adhesive
 - 2.2.4 Panel Construction
- 2.3 COMMON PANEL REQUIREMENTS
 - 2.3.1 Appearance
 - *AM0003 2.3.2 Panel Fabrication AM0003*
 - 2.3.3 Condensation Index Rating
- *AM0003 2.4 TRANSLUCENT PANEL SYSTEMS AM0003*
- 2.5 FLEXIBLE SEALING TAPE

PART 3 EXECUTION

- 3.1 EXAMINATION
- 3.2 ERECTION

-- End of Section Table of Contents --

SECTION 08 60 45
TRANSLUCENT PANELS

PART 1 GENERAL

1.1 SUMMARY

Provide commercially available translucent panels which satisfy all requirements contained in this section and have been verified by load testing and independent design analyses (if required) to meet specified design requirements. Provide UV-stabilized, shatterproof and energy efficient skylight systems. Provide light transmitting plastics in the manufacturing of skylights for daylighting applications. Systems must meet requirements of **UFC 4-010-01**.

1.2 REFERENCES

The publications listed below form a part of this specification to the extent referenced. The publications are referred to within the text by the basic designation only.

AMERICAN ARCHITECTURAL MANUFACTURERS ASSOCIATION (AAMA)

AAMA 2605	(2020) Voluntary Specification, Performance Requirements and Test Procedures for Superior Performing Organic Coatings on Aluminum Extrusions and Panels
AAMA/WDMA/CSA 101/I.S.2/A440	(2017) North American Fenestration Standard/Specification for Windows, Doors, and Skylights

ASTM INTERNATIONAL (ASTM)

ASTM C297/C297M	(2016) Flatwise Tensile Strength of Sandwich Constructions
ASTM D572	(2004; R 2019) Rubber Deterioration by Heat and Oxygen
ASTM D1002	(2010; R 2019) Apparent Shear Strength of Single-Lap-Joint Adhesively Bonded Metal Specimens by Tension Loading (Metal-to-Metal)
ASTM D1003	(2013) Haze and Luminous Transmittance of Transparent Plastics
ASTM D1037	(2012; R 2020) Standard Test Methods for Evaluating Properties of Wood-Base Fiber and Particle Panel Materials
ASTM D3841	(2016) Standard Specification for Glass Fiber-Reinforced Polyester Plastic Panels
ASTM E72	(2022) Conducting Strength Tests of Panels for Building Construction
ASTM E108	(2020a) Standard Test Methods for Fire Tests of Roof Coverings

ASTM E283	(2019) Standard Test Method for Determining the Rate of Air Leakage Through Exterior Windows, Curtain Walls, and Doors Under Specified Pressure Differences Across the Specimen
ASTM E331	(2000; R 2023) Standard Test Method for Water Penetration of Exterior Windows, Skylights, Doors, and Curtain Walls by Uniform Static Air Pressure Difference
ASTM E661	(2022) Standard Test Method for Performance of Wood and Wood-Based Floor and Roof Sheathing Under Concentrated Static and Impact Loads
ASTM E695	(2022) Standard Test Method of Measuring Relative Resistance of Wall, Floor, and Roof Construction to Impact Loading
ICC EVALUATION SERVICE, INC. (ICC-ES)	
ICC-ES AC04	(2012; R 2015) Acceptance Criteria for Sandwich Panels
INTERNATIONAL CODE COUNCIL (ICC)	
ICC IBC	(2021) International Building Code
NATIONAL FENESTRATION RATING COUNCIL (NFRC)	
NFRC 100	(2020) Procedure for Determining Fenestration Product U-Factors
NFRC 200	(2020) Procedure for Determining Fenestration Product Solar Heat Gain Coefficient and Visible Transmittance at Normal Incidence
U.S. DEPARTMENT OF DEFENSE (DOD)	
UFC 4-010-01	(2018; with Change 3, 2024) DoD Minimum Antiterrorism Standards for Buildings
U.S. NATIONAL ARCHIVES AND RECORDS ADMINISTRATION (NARA)	
29 CFR 1910.23	(Nov 2016) Ladders
UNDERWRITERS LABORATORIES (UL)	
UL 972	(2006; Reprint Nov 2020) UL Standard for Safety Burglary Resisting Glazing Material Type

1.3 SUBMITTALS

Government approval is required for submittals with a "G" or "S" classification. Submittals not having a "G" or "S" classification are for information only. When used, a code following the "G" classification identifies the office that will review the submittal for the Government. Submit the following in accordance with Section 01 33 00 SUBMITTAL PROCEDURES:

SD-02 Shop Drawings

Shop Drawings; G, DO

SD-03 Product Data

Translucent Panels; G, DO

Recycled Content for Aluminum Framing Materials; S

Warranty; G, DO

SD-06 Test Reports; G, DO

Test Reports

SD-07 Certificates

Systems

Qualifications

1.4 QUALITY ASSURANCE

- a. Provide documentation of **Qualifications** for the following: The manufacturer is a company specializing in the manufacture of the specified products with a minimum of 5 years documented experience. The installer has documented experience of 5 years minimum performing the work specified.

1.5 DELIVERY, STORAGE, AND HANDLING

Provide factory assembled system modules to the greatest extent possible. Ship panels to the jobsite in rugged shipping units, ready for erection. Affix conspicuous decals on all skylights warning individuals against sitting or stepping on the units. Store skylight panels on the long edge, several **inches** above the ground, blocked and under cover to prevent warping. Deliver unit skylights in manufacturer's original containers, dry, undamaged, with seals and labels intact. Deliver, store and protect all products in accordance with manufacturer's recommendations.

1.6 WARRANTY

Provide the manufacturer's complete warranty for materials, workmanship, and installation. The warranty is for 5 years from the time of project completion and with no proration. The warranty must guarantee, but not be limited to, the following:

- a. No change in light transmission and color of the panels after exposure to heat of **300 degrees F** for 25 minutes.
- b. There is no delamination of the panel affecting appearance, performance, weatherability or structural integrity of the panels or the completed system.
- c. There is no fiberbloom on the panel face.
- d. Change in light transmission of no more than 6 percent in accordance with **ASTM D1003**, and in color (yellowing index) no more than 10 points in comparison to the original specified value over a 10 year period.
- e. Provide a single source warranty for the glazing panels and the framing system. Third party warranty for the glazing panels will not be accepted.

PART 2 PRODUCTS

2.1 TRANSLUCENT PANELS

Fabricate skylight panels of glass-fiber reinforced polyester panels conforming to the specified requirements and other appropriate lab test specified criteria, weighing not less than **8 ounces/square foot**. Submit certified **Test Reports** from independent testing laboratory for each type and class of panel system. Reports must verify that the material meets specified performance requirements. Previously completed test reports will be acceptable if they are current and indicative of products used on this project. Where a Class A, B or C roof is part of the project, provide a listing certificate for roof covering systems category certifying that the product complies with the safety standards of **ASTM E108** and **ICC IBC**. Size and color of skylight panels as indicated.

2.2 GLASS-FIBER PANELS

Provide glass-fiber reinforced polyester panels conforming to **ASTM D3841**, Class CC2 and to the requirements of **AAMA/WDMA/CSA 101/I.S.2/A440**.

2.2.1 Weatherability

Provide the exposed faces of fiberglass sandwich type panels with a permanent glass veil erosion barrier embedded integrally to provide maximum long term resistance to reinforcing fiber exposure. The exterior face sheet must be uniform in strength and resistant to penetration by pencil point.

2.2.2 Non Combustible Grid Core

Use 6063-T6 aluminum I-beams with provisions for mechanical interlocking of muntin-mullion and perimeter to prevent high and low intersections which do not allow full bonding surface to contact with face material. I-beam width no less than **7/16 inch**. Machine I-beam grid to tolerances of not greater than plus or minus **0.002 inch** for flat panels. Panels must withstand **1200 degrees F** fire for a minimum of one hour without collapse or exterior flaming.

2.2.3 Adhesive

Use heat and pressure resin-type laminate adhesive engineered for structural sandwich panel use; which passes testing requirements specified by the International Conference of Building Officials' "Acceptance Criteria for Sandwich Panel Adhesive". Provide with the following minimum strength:

- a. Tensile Strength of **750 psi** in accordance with **ASTM C297/C297M** after two exposures to six cycles each of the aging conditions prescribed in **ASTM D1037**.
- b. Shear Strength, after exposure to five separate aging conditions in accordance with **ASTM D1002**:
 - (1) **540 psi** at 50 percent relative humidity and **73 degrees F**.
 - (2) **800 psi** under accelerated aging in accordance with **ASTM D1037** at room temperature.
 - (3) **250 psi** under accelerated aging in accordance with **ASTM D1037** at **182 degrees F**.
 - (4) **1400 psi** after 500 hour Oxygen Bomb in accordance with **ASTM D572**.
 - (5) **100 psi** at **182 degrees F**.

2.2.4 Panel Construction

Provide panels consisting of fiberglass faces laminated to an aluminum I-beam grid core and deflecting no more than **1.9 inches** at **30 psf in 10 feet** in accordance with **ASTM E72**, without a supporting frame. Include manufacturing facilities, sandwich panel components and production sandwich panels in the quality control inspections and required testing, conducted at least once each year, for

conformance with ICC-ES AC04 or equivalent. Provide aluminum framing materials with a minimum recycled content of 20 percent. Provide data identifying percentage of recycled content for aluminum framing materials.

2.3 COMMON PANEL REQUIREMENTS

2.3.1 Appearance

Provide face sheets uniform in color to prevent splotchy appearance and completely free of ridges and wrinkles which prevent proper surface contact. Clusters of air bubbles/pinholes which collect moisture and dirt are not acceptable.

2.3.2 Panel Fabrication

Panel construction must meet the following requirements:

- a. Light transmission 30 percent; exterior color crystal; interior color crystal..
- b. Assembled panel thickness 2 3/4 inches.

*AM0003 c. Grid size nominal 42 24 inches x 24 12 inches.

AM0003*

2.3.3 Condensation Index Rating

The condensation index rating must be 26 as determined using National Fenestration Rating Council approved software THERM.

2.4 TRANSLUCENT PANEL SYSTEMS

Submit manufacturer's certificate that the systems meet or exceed specified requirements. Provide systems evaluated and listed (the whole translucent panel as a unit, not just a glazing material in the unit) by the recognized building code authorities: ICC and SBCCI-Public Safety Testing and Evaluation Services Inc. Product ratings determined using NFRC 100 and NFRC 200 must be authorized for certification and properly labeled by the manufacturer. Provide translucent panel systems meeting the following requirements:

- *AM0003 a. Thermally broken, integral perimeter framing system assembly by the manufacturer. AM0003*
- b. Exterior panel faces white in color. Interior panel faces white in color.
- c. Air infiltration at 1.57 psf less than 0.04 cfm/ft² and at 6.24 psf less than 0.07 cfm/ft² in accordance with ASTM E283.
- d. Water penetration at test pressure of 15 psf equals zero in accordance with ASTM E331.
- e. Manufacturer is responsible for maximum system deflection, in accordance with the applicable building code, and without damage to system performance. Calculate deflection in accordance with engineering principles.
- f. Incorporate weepage elements within the perimeter framework of the glazing system for drainage of any condensation or water penetration.
- g. System must accommodate movement within the system; movement between the system and perimeter framing components; dynamic loading and release of loads; and deflection of supporting members. Achieve this without damage to system or components, deterioration of weather seals and fenestration properties specified.
- h. The exterior panel face must repel an impact of 50 foot-pounds without fracture or tear when impacted by a 3.25 inch diameter, 5 pound free falling ball dropped from a vertical distance of 10

feet when tested in accordance with UL 972.

- i. Provide system meeting the fall through requirements of 29 CFR 1910.23 as demonstrated by testing in accordance with ASTM E661 or ASTM E695, thereby not requiring supplemental screens or railings.
- j. Exposed aluminum color must be selected from the manufacturer's standard range. Provide corrosion resistant superior-performance organic finish in accordance with AAMA 2605.
- k. Provide a system requiring no scheduled recoating to maintain its performance or for UV resistance.
- l. Design criteria:
 - (1) Wind Load 114 mph; snow load 7 psf.
 - (2) Frame Blast Loads: Design framing to resist 50 pounds per square foot blast load at L/160 deflection.
 - (3) Anchor Blast Loads: Design anchors to resist 100 pounds per square foot blast load.
- m. Use 6063-T6 and 6063-T5 extruded aluminum; all fasteners of stainless steel or plated steel.

*AM0003 n. U-Value to meet or exceed .29 (Btu/hr/ft²/°F).

AM0003*

2.5 FLEXIBLE SEALING TAPE

Provide manufacturer's standard pre-applied sealing tape to closure system at the factory under controlled conditions.

PART 3 EXECUTION

3.1 EXAMINATION

Field verify all submitted opening sizes, dimensions and tolerances; preparation of openings includes isolating dissimilar materials from aluminum system to avoid damage by electrolysis. The installer must examine area of installation to verify readiness of site conditions and to notify the Contractor about any defects requiring correction. Verify when structural support is ready to receive all specified work and to convene a pre-installation conference, if approved by the Contracting Officer, including the Contractor, skylight installer and all parties directly affecting and affected by the specified work. Do not install any materials that show visual evidence of biological growth due to the presence of moisture. Do not commence work until conditions are satisfactory.

3.2 ERECTION

Erect translucent skylight system in accordance with the approved shop drawings supplied by the manufacturer. Submit drawings showing fabrication details, materials, dimensions, installation methods, anchors, and relationship to adjacent construction. Fasten and seal in accordance with the manufacturer's shop drawings. Remove all panel, after other trades have completed work on adjacent materials. Carefully inspect and adjust panel installation as necessary to ensure proper installation and weather-tight conditions. provide all staging, lifts and hoists required for the complete installation and field measuring. Install system clean of dirt, debris or staining and thoroughly examined for removal of all protective material prior to final inspection of the designated work area. Do not use snow rakes on roof windows or skylights.

-- End of Section --

SECTION TABLE OF CONTENTS

DIVISION 08 - OPENINGS

SECTION 08 71 00

DOOR HARDWARE

PART 1 GENERAL

- 1.1 REFERENCES
- 1.2 SUBMITTALS
- 1.3 SHOP DRAWINGS
- 1.4 PRODUCT DATA
- 1.5 HARDWARE SCHEDULE
 - 1.5.1 Hardware Item List:
 - 1.5.2 Hardware Schedule
- 1.6 KEY BITTING CHART REQUIREMENTS
 - 1.6.1 Requirements
- 1.7 QUALITY ASSURANCE
 - 1.7.1 Hardware Manufacturers and Modifications
 - 1.7.2 Key Shop Drawings Coordination Meeting
- 1.8 DELIVERY, STORAGE, AND HANDLING

PART 2 PRODUCTS

- 2.1 TEMPLATE HARDWARE
- 2.2 HARDWARE FOR FIRE DOORS AND EXIT DOORS
- 2.3 HARDWARE ITEMS
 - 2.3.1 Hinges
 - 2.3.2 Locks and Latches
 - 2.3.2.1 Mortise Locks and Latches
 - 2.3.2.2 Bored Locks and Latches
 - 2.3.2.3 Auxiliary Locks
 - 2.3.3 Exit Devices
 - 2.3.4 Cylinders and Cores
 - 2.3.5 Electrified Hardware
 - 2.3.5.1 Electric Strikes and Frame Mounted Actuators
 - 2.3.5.1.1 Solenoid
 - 2.3.5.1.2 Signal Switches
 - 2.3.5.1.3 Tamper Resistance
 - 2.3.5.1.4 Coordination
 - 2.3.5.1.5 Mounting Method
 - 2.3.5.2 Electrified Mortise Locks
 - 2.3.5.2.1 Power Transfer Hinge and Electric Power Transfers (EPT)s
 - 2.3.5.3 Card Reader Access Control Hardware
 - 2.3.5.4 Release Devices
 - 2.3.5.4.1 Release Devices
 - 2.3.5.5 Power Assist and Low Energy Power Operated Doors
 - 2.3.5.6 Electromagnetic Locks
 - 2.3.5.6.1 Armature
 - 2.3.5.6.2 Tamper Resistance
 - 2.3.5.6.3 Mounting Method
 - 2.3.5.7 Delayed Egress Locking System

- 2.3.5.8 Power and Manual Operated Revolving Pedestrian Doors
- 2.3.6 Keying System
- 2.3.7 Lock Trim
 - 2.3.7.1 Knobs and Roses
 - 2.3.7.2 Lever Handles
- 2.3.8 Keys
- 2.3.9 Door Bolts
- 2.3.10 Closers
 - 2.3.10.1 Identification Marking
- 2.3.11 Overhead Holders
- 2.3.12 Door Protection Plates
 - 2.3.12.1 Sizes of Kick Plates
- 2.3.13 Door Stops and Silencers
- 2.3.14 Padlocks
- 2.3.15 Thresholds
- 2.3.16 Weatherstripping Gasketing
 - 2.3.16.1 Extruded Aluminum Retainers
 - 2.3.16.2 Interlocking Type
 - 2.3.16.3 Spring Tension Type
- 2.3.17 Soundproofing Gasketing
- 2.3.18 Rain Drips
 - 2.3.18.1 Door Rain Drips
 - 2.3.18.2 Overhead Rain Drips
- 2.3.19 Auxiliary Hardware (Other than locks)
- 2.3.20 Sliding and Folding Door Hardware
- 2.3.21 Special Tools
- 2.4 FASTENERS
- 2.5 FINISHES
- 2.6 KEY CABINET AND CONTROL SYSTEM

PART 3 EXECUTION

- 3.1 INSTALLATION
 - 3.1.1 Weatherstripping Installation
 - 3.1.1.1 Stop Applied Weatherstripping
 - 3.1.1.2 Interlocking Type Weatherstripping
 - 3.1.1.3 Spring Tension Type Weatherstripping
 - 3.1.2 Soundproofing Installation
 - 3.1.3 Threshold Installation
- 3.2 FIRE DOORS AND EXIT DOORS
- 3.3 HARDWARE LOCATIONS
- 3.4 KEY CABINET AND CONTROL SYSTEM
- 3.5 FIELD QUALITY CONTROL
- AM0003* 3.6 HARDWARE SETS *AM0003

-- End of Section Table of Contents --

SECTION 08 71 00

DOOR HARDWARE

PART 1 GENERAL

1.1 REFERENCES

The publications listed below form a part of this specification to the extent referenced. The publications are referred to within the text by the basic designation only.

ASTM INTERNATIONAL (ASTM)

ASTM E283 (2019) Standard Test Method for Determining the Rate of Air Leakage Through Exterior Windows, Curtain Walls, and Doors Under Specified Pressure Differences Across the Specimen

ASTM F883 (2013; R 2022) Standard Performance Specification for Padlocks

BUILDERS HARDWARE MANUFACTURERS ASSOCIATION (BHMA)

ANSI/BHMA A156.1 (2021) Butts and Hinges

ANSI/BHMA A156.2 (2022) Bored and Preassembled Locks and Latches

ANSI/BHMA A156.3 (2020) Exit Devices

ANSI/BHMA A156.4 (2024) Door Controls - Closers

ANSI/BHMA A156.5 (2020) Cylinder and Input Devices for Locks

ANSI/BHMA A156.6 (2021) Architectural Door Trim

ANSI/BHMA A156.7 (2016) Template Hinge Dimensions

ANSI/BHMA A156.8 (2021) Door Controls - Overhead Stops and Holders

ANSI/BHMA A156.13 (2022) Mortise Locks & Latches Series 1000

ANSI/BHMA A156.14 (2013) Sliding and Folding Door Hardware

ANSI/BHMA A156.15 (2021) Release Devices Closer Holder, Electromagnetic and Electromechanical

ANSI/BHMA A156.16 (2023) Auxiliary Hardware

ANSI/BHMA A156.18 (2020) Materials and Finishes

ANSI/BHMA A156.19 (2013) Power Assist & Low Energy Power Operated Doors

ANSI/BHMA A156.21 (2019) Thresholds

ANSI/BHMA A156.22 (2021) Gasketing

ANSI/BHMA A156.23	(2010) Electromagnetic Locks
ANSI/BHMA A156.24	(2012) Delayed Egress Locking Systems
ANSI/BHMA A156.25	(2013) Electrified Locking Devices
ANSI/BHMA A156.27	(2011) Power and Manual Operated Revolving Pedestrian Doors
ANSI/BHMA A156.31	(2013) Electric Strikes and Frame Mounted Actuators
ANSI/BHMA A156.36	(2010) Auxiliary Locks

NATIONAL FIRE PROTECTION ASSOCIATION (NFPA)

NFPA 70	(2023; ERTA 1 2024; TIA 24-1) National Electrical Code
NFPA 72	(2022; ERTA 22-1) National Fire Alarm and Signaling Code
NFPA 80	(2022) Standard for Fire Doors and Other Opening Protectives
NFPA 101	(2024) Life Safety Code
NFPA 252	(2022) Standard Methods of Fire Tests of Door Assemblies

STEEL DOOR INSTITUTE (SDI/DOOR)

SDI/DOOR A250.8	(2023) Specifications for Standard Steel Doors and Frames
-----------------	---

U.S. NATIONAL ARCHIVES AND RECORDS ADMINISTRATION (NARA)

36 CFR 1191	Americans with Disabilities Act (ADA) Accessibility Guidelines for Buildings and Facilities; Architectural Barriers Act (ABA) Accessibility Guidelines
-------------	--

UNDERWRITERS LABORATORIES (UL)

UL Bld Mat Dir	(updated continuously online) Building Materials Directory
----------------	--

1.2 SUBMITTALS

Government approval is required for submittals with a "G" or "S" classification. Submittals not having a "G" or "S" classification are for information only. When used, a code following the "G" classification identifies the office that will review the submittal for the Government. Submit the following in accordance with Section 01 33 00 SUBMITTAL PROCEDURES:

SD-02 Shop Drawings

- Manufacturer's Detail Drawings; G, DO
- Verification of Existing Conditions; G, DO
- Hardware Schedule; G, DO
- Keying System; G, DO

SD-03 Product Data

Hardware Items; G, DO

SD-08 Manufacturer's Instructions

Installation

SD-10 Operation and Maintenance Data

Hardware Schedule Items, Data Package 1; G, DO

SD-11 Closeout Submittals

Key Bitting

1.3 SHOP DRAWINGS

Submit [manufacturer's detail drawings](#) indicating all hardware assembly components and interface with adjacent construction. Indicate power components and wiring coordination for electrified hardware. Base shop drawings on verified field measurements and include [verification of existing conditions](#).

1.4 PRODUCT DATA

Indicate fire-ratings at applicable components. Provide documentation of ABA/ADA accessibility compliance of applicable components, as required by [36 CFR 1191](#) Appendix D - Technical.

1.5 HARDWARE SCHEDULE

Provide Hardware Item List and Hardware Schedule containing the following information, and additional information as needed to identify the complete make up of each hardware set and its application to each opening:

1.5.1 Hardware Item List:

- a. Hardware Type
- b. Item Number
- c. Quantity
- d. Size(s)
- e. Reference Publication / Type Number
- f. Manufacturer's Name / Catalog Number
- g. Key Control Symbols
- h. UL Mark (If fire rated and listed)
- i. BHMA Finish(es)
- j. Remarks

1.5.2 Hardware Schedule

- a. Hardware Set Number
- b. Opening Number(s)

- c. Opening Description (single/double leaf, hand, size, door/frame material)
- d. Fire Rating
- e. Sound Rating
- f. Hardware Items
- g. Quantity
- h. Size
- i. BHMA Finish
- j. Remarks

In addition, submit hardware schedule data package 1 in accordance with Section 01 78 23 OPERATION AND MAINTENANCE DATA.

1.6 KEY BITTING CHART REQUIREMENTS

1.6.1 Requirements

Submit **key bitting** charts to the Contracting Officer prior to completion of the work. Include:

- a. Complete listing of all keys (e.g. AA1 and AA2).
- b. Complete listing of all key cuts (AA1-123456, AA2-123458).
- c. Tabulation showing which key fits which door.
- d. Copy of floor plan showing doors and door numbers.
- e. Listing of 20 percent more key cuts than are presently required in each master system.

1.7 QUALITY ASSURANCE

1.7.1 Hardware Manufacturers and Modifications

Provide, as far as feasible, locks, hinges, and closers of one lock, hinge, or closer manufacturer's make. Modify hardware as necessary to provide features indicated or specified.

1.7.2 Key Shop Drawings Coordination Meeting

Prior to the submission of the key shop drawing, the Contracting Officer, Contractor, Door Hardware Subcontractor, using Activity and Base Locksmith must meet to discuss and coordinate key requirements for the facility.

1.8 DELIVERY, STORAGE, AND HANDLING

Deliver hardware in original individual containers, complete with necessary appurtenances including fasteners and instructions. Mark each individual container with item number as shown on hardware schedule. Deliver permanent keys to the Contracting Officer, either directly or by certified mail. Deliver construction master keys with the locks.

PART 2 PRODUCTS

2.1 TEMPLATE HARDWARE

Hardware applied to metal or to prefinished doors must be manufactured using a template. Provide templates to door and frame manufacturers in accordance with [ANSI/BHMA A156.7](#) for template hinges. Coordinate hardware items to prevent interference with other hardware.

2.2 HARDWARE FOR FIRE DOORS AND EXIT DOORS

Provide all hardware necessary to meet the requirements of [NFPA 72](#) for door alarms, [NFPA 80](#) for fire doors, [NFPA 101](#) for exit doors, [NFPA 252](#) for fire tests of door assemblies, ABA/ADA accessibility requirements, and all other requirements indicated, even if such hardware is not specifically mentioned in paragraph HARDWARE SCHEDULE. Provide Underwriters Laboratories, Inc. labels for such hardware in accordance with [UL Bld Mat Dir](#) or equivalent labels in accordance with another testing laboratory approved in writing by the Contracting Officer.

2.3 HARDWARE ITEMS

Clearly and permanently mark with the manufacturer's name or trademark, hinges, pivots, locks, latches, exit devices, bolts and closers where the identifying mark is visible after the item is installed. For closers with covers, the name or trademark may be beneath the cover. Coordinate electrified door hardware components with corresponding components specified in Division 28 ELECTRONIC SECURITY SYSTEMS (ESS).

2.3.1 Hinges

Provide in accordance with [ANSI/BHMA A156.1](#). Provide hinges that are [4-1/2 by 4-1/2 inch](#) unless otherwise indicated. Construct loose pin hinges for interior doors and reverse-bevel exterior doors so that pins are non-removable when door is closed. Other anti-friction bearing hinges may be provided in lieu of ball bearing hinges.

2.3.2 Locks and Latches

- a. At exterior locations provide locksets of full stainless steel type 302 or 304 construction including fronts, strike, escutcheons, knobs, bolts and all interior working parts. Marine Grade I, fully non-ferrous.
- b. In non-air-conditioned interior environments or humid interior environments, provide interior locksets on the same Marine Grade I, fully non-ferrous as exterior locksets.

2.3.2.1 Mortise Locks and Latches

Provide in accordance with [ANSI/BHMA A156.13](#), Series 1000, Operational Grade 1, Security Grade 2. Provide mortise locks with escutcheons not less than [7 by 2-1/4 inch](#) with a bushing at least [1/4 inch](#) long. Cut escutcheons to fit cylinders and provide trim items with straight, beveled, or smoothly rounded sides, corners, and edges. Provide knobs and roses of mortise locks with screwless shanks and no exposed screws.

2.3.2.2 Bored Locks and Latches

Provide in accordance with [ANSI/BHMA A156.2](#), Series 4000, Grade 1.

2.3.2.3 Auxiliary Locks

Provide in accordance with [ANSI/BHMA A156.36](#), Grade 1.

2.3.3 Exit Devices

Provide in accordance with [ANSI/BHMA A156.3](#), Grade 1. Provide adjustable strikes for rim type and

vertical rod devices. Provide open back strikes for pairs of doors with mortise and vertical rod devices. Provide touch bars in lieu of conventional crossbars and arms. Provide escutcheons not less than 7 by 2-1/4 inch.

2.3.4 Cylinders and Cores

Provide cylinders and cores for new locks, including locks provided under other sections of this specification. Provide cylinders and cores with pin tumblers to match key system. Provide cylinders from the products of one manufacturer, and provide cores from the products of one manufacturer. Rim cylinders and mortise cylinders have interchangeable cores which are removable by special control keys. Stamp each interchangeable core with a key control symbol in a concealed place on the core.

2.3.5 Electrified Hardware

Comply with the requirements of NFPA 70 for wiring of electrified hardware.

2.3.5.1 Electric Strikes and Frame Mounted Actuators

Provide in accordance with ANSI/BHMA A156.31, Grade 1. Provide electric strikes and actuators as required to meet operational requirements. Provide electric strikes that remain secure during power failure. Provide a separate power supply for electric strikes, other locking devices and ancillary parts. Provide battery backup for continued operation during power failure. Provide strikes and actuators with a minimum opening force of 2300 pounds.

Provide facility interface devices that use direct current (dc) power to energize the solenoids. Provide electric strikes and actuators that incorporate end-of-line resistors to facilitate line supervision by the system. If not incorporated into the electric strike or local controller, provide metal oxide resistors (MOVs) to protect the controller from reverse current surges.

2.3.5.1.1 Solenoid

Provide actuating solenoid for strikes and actuators that are rated for continuous duty, cannot dissipate more than 12 Watts and must operate on 12 or 24 Volts dc. Inrush current cannot exceed 1 ampere and the holding current cannot be greater than 500 milliamperes. Actuating solenoid must move from fully secure to fully open positions in less than 500 milliseconds.

2.3.5.1.2 Signal Switches

Provide strikes and actuators with signal switches to indicate to the system when the bolt is not engaged or the strike mechanism is unlocked. Signal switches must report a forced entry to the system.

2.3.5.1.3 Tamper Resistance

Provide strike guards that prevent tampering with the latch bolt of the locking hardware or the latch bolt keeper of the electric strike. Strike guards to bolt through the door using tamper resistant screws. Provide strike guards made of 1/8 inch thick brass and that are 11-1/14 inch high by 1-5/8 inch wide, with a minimum 5/32 inch wide offset.

2.3.5.1.4 Coordination

Provide electric strikes and actuators of a size, weight and profile compatible with each specified door frame. Field verify installation clearances prior to procurement.

2.3.5.1.5 Mounting Method

Provide electric strikes and actuators suitable for use with single and double doors, with mortise or rim type hardware specified, and for right or left hand mounting as specified. In double door installations, locate the lock in the active leaf and monitor the fixed leaf.

2.3.5.2 Electrified Mortise Locks

Provide in accordance with [ANSI/BHMA A156.25](#), Grade 1. Provide electrified mortise locks that remain secure during power failure. Provide facility interface devices that use dc power to energize solenoids. Provide solenoids, resisters, and signal switches in accordance with paragraph ELECTRIC STRIKES AND FRAME MOUNTED ACTUATORS.

2.3.5.2.1 Power Transfer Hinge and Electric Power Transfers (EPT)s

Provide power transfer hinges with each electrified lock or EPTs that route power and monitoring signals from the lockset to the door frame. Coordinate power transfer devices with door frames.

2.3.5.3 Card Reader Access Control Hardware

Provide in accordance with [ANSI/BHMA A156.5](#) and [ANSI/BHMA A156.25](#), Grade 1 components. Provide devices that are tamper alarmed, tamper and vandal resistant, solid state, and do not contain electronics which could compromise the access control subsystem should the subsystem be attacked. Provide surface, semi-flush, pedestal, or weatherproof mountable devices as specified for each individual location. Provide proximity type card readers capable of reading proximity Keypad type access control cards. Coordinate access control hardware with corresponding devices and systems specified in Division 28 ELECTRONIC SECURITY SYSTEMS (ESS).

2.3.5.4 Release Devices

In accordance with [ANSI/BHMA A156.15](#), Grade 1.

2.3.5.4.1 Release Devices

Provide wall mounted Electromagnetic release devices connected to fire detecting devices.

2.3.5.5 Power Assist and Low Energy Power Operated Doors

Provide in accordance with [ANSI/BHMA A156.19](#), Grade 1.

2.3.5.6 Electromagnetic Locks

Provide in accordance with [ANSI/BHMA A156.23](#), Grade 1. Provide electromagnetic locks that do not contain any moving parts and depend solely upon electromagnetism to secure a portal by generating at least **1200 pounds** of holding force. The lock must interface with the local processors without external, internal or functional alteration of the local processor. The electromagnetic lock must incorporate an end of line resistor to facilitate line supervision by the system. Provide metal-oxide resistors (MOVs) to protect controllers from reverse current surges, if not incorporated into the electromagnetic lock or local controller.

2.3.5.6.1 Armature

Provide electromagnetic locks with internal circuitry to eliminate residual magnetism and inductive kickback. Provide actuating armature that operates on 12 or 24 Volts dc and cannot dissipate more than 12 Watts. Holding current must be less than 500 milliamperes. Actuating armature must take less than 300 milliseconds to change the status of the lock from fully secure to fully open or fully open to fully secure.

2.3.5.6.2 Tamper Resistance

Provide lock mechanism encased in hardened guard barriers to deter forced entry.

2.3.5.6.3 Mounting Method

Provide electromagnetic lock suitable for use with single and double door with mortise or rim type hardware and compatible with right or left hand mounting.

2.3.5.7 Delayed Egress Locking System

Provide in accordance with [ANSI/BHMA A156.24](#), Grade 1.

2.3.5.8 Power and Manual Operated Revolving Pedestrian Doors

Provide in accordance with [ANSI/BHMA A156.27](#), Grade 1.

2.3.6 Keying System

Provide an extension of the existing keying system. Provide key cabinet as specified.

2.3.7 Lock Trim

Provide cast, forged, or heavy wrought construction and commercial plain design for lock trim.

2.3.7.1 Knobs and Roses

Provide in accordance with [ANSI/BHMA A156.2](#) and [ANSI/BHMA A156.13](#) for knobs, roses, and escutcheons. For unreinforced knobs, roses, and escutcheons, provide a [0.050 inch](#) thickness. For reinforced knobs, roses, and escutcheons, provide an outer shell thickness of [0.035 inch](#) and a combined total thickness of [0.070 inch](#), except at knob shanks. Provide knob shanks [0.060 inch](#) thick.

2.3.7.2 Lever Handles

Provide lever handles where indicated in the Hardware Schedule. Provide in accordance with [ANSI/BHMA A156.3](#) for mortise locks of lever handles for exit devices. Provide lever handle locks with a breakaway feature (such as a weakened spindle or a shear key) to prevent irreparable damage to the lock when force in excess of that specified in [ANSI/BHMA A156.13](#) is applied to the lever handle. Provide lever handles return to within [1/2 inch](#) of the door face.

2.3.8 Keys

Provide one file key, one duplicate key, and one working key for each key change and for each master and grand master keying system. Provide one additional working key for each lock of each keyed-alike group. Provide 4 great grand master keys, 8 construction master keys, and 2 control keys for removable cores. Provide a quantity of key blanks equal to 20 percent of the total number of file keys. Stamp each key with appropriate key control symbol and "U.S. property - do not duplicate." Do not place room number on keys.

2.3.9 Door Bolts

Provide in accordance with [ANSI/BHMA A156.16](#). Provide dustproof strikes for bottom bolts, except at doors having metal thresholds. Provide automatic latching flush bolts in accordance with [ANSI/BHMA A156.3](#), Type 25.

2.3.10 Closers

Provide in accordance with [ANSI/BHMA A156.4](#), Series C02000, Grade 1, with PT 4C. Provide with brackets, arms, mounting devices, fasteners, full size covers, except at storefront mounting, and other features necessary for the particular application. Size closers in accordance with manufacturer's printed recommendations, or provide multi-size closers, Sizes 1 through 6, and list sizes in the Hardware Schedule. Provide manufacturer's 10 year warranty.

Use stainless steel inside bracketed or door mounted closers on exterior doors. Non-ferrous closers, such as aluminum or cast bronze, are permissible where door utilization is minimal. On interior doors use closers of 302 or 304 stainless steel or non-ferrous materials. On surface-mounted closers use or apply rust inhibiting finish on all ferrous parts. Also apply this finish on concealed closers.

2.3.10.1 Identification Marking

Engrave each closer with manufacturer's name or trademark, date of manufacture, and manufacturer's size designation in locations that will be visible after installation.

2.3.11 Overhead Holders

Provide in accordance with [ANSI/BHMA A156.8](#).

2.3.12 Door Protection Plates

Provide in accordance with [ANSI/BHMA A156.6](#).

2.3.12.1 Sizes of Kick Plates

[2 inch](#) less than door width for single doors; [1 inch](#) less than door width for pairs of doors. Provide [10 inch](#) kick plates for flush doors .

2.3.13 Door Stops and Silencers

Provide in accordance with [ANSI/BHMA A156.16](#). Silencers Type L03011. Provide three silencers for each single door, two for each pair.

2.3.14 Padlocks

Provide in accordance with [ASTM F883](#).

2.3.15 Thresholds

Provide in accordance with [ANSI/BHMA A156.21](#). Use J35100, with vinyl or silicone rubber insert in face of stop, for exterior doors opening out, unless specified otherwise.

2.3.16 Weatherstripping Gasketing

Provide in accordance with [ANSI/BHMA A156.22](#). Provide the type and function designation where specified in paragraph HARDWARE SCHEDULE. Provide a set to include head and jamb seals, sweep strips, and, for pairs of doors, astragals. Air leakage of weatherstripped doors not to exceed [1.25 cubic feet](#) per minute of air per square [foot](#) of door area when tested in accordance with [ASTM E283](#). Provide weatherstripping with one of the following:

2.3.16.1 Extruded Aluminum Retainers

Extruded aluminum retainers not less than [0.050 inch](#) wall thickness with vinyl, neoprene, silicone rubber, or polyurethane inserts. Provide clear (natural) anodized aluminum.

2.3.16.2 Interlocking Type

Zinc or bronze not less than [0.018 inch](#) thick.

2.3.16.3 Spring Tension Type

Spring bronze or stainless steel not less than [0.008 inch](#) thick.

2.3.17 Soundproofing Gasketing

Provide in accordance with [ANSI/BHMA A156.22](#). Provide adjustable doorstops at heads, jambs and automatic door bottoms in accordance with the hardware set, of extruded aluminum, clear (natural) anodized, surface applied, with vinyl fin seals between plunger and housing. Provide doorstops with solid neoprene tube, silicone rubber, or closed cell sponge gasket. Provide door bottoms with adjustable operating rod and silicone rubber or closed cell sponge neoprene gasket. Provide doorstops that are mitered at corners. Provide type and function designation where specified in paragraph HARDWARE SETS.

2.3.18 Rain Drips

Provide in accordance with [ANSI/BHMA A156.22](#). Provide extruded aluminum rain drips, not less than [0.08 inch](#) thick, clear anodized finish. Provide the manufacturer's full range of color choices to the Contracting Officer for color selection. Provide rain drips with a [4 inch](#) overlap on each side of each exterior door that is not protected by an awning, roof, eave or other horizontal projection. Set drips in sealant and fasten with stainless steel screws.

2.3.18.1 Door Rain Drips

Approximately [1-1/2 inch high by 5/8 inch](#) projection. Align bottom with bottom edge of door.

2.3.18.2 Overhead Rain Drips

Approximately [1-1/2 inch high by 2-1/2 inch](#) projection. Align bottom with door frame rabbet.

2.3.19 Auxiliary Hardware (Other than locks)

Provide in accordance with [ANSI/BHMA A156.16](#), Grade 1.

2.3.20 Sliding and Folding Door Hardware

Provide in accordance with [ANSI/BHMA A156.14](#), Grade 1. Finishes to match other hardware specified herein.

2.3.21 Special Tools

Provide special tools, such as spanner and socket wrenches and dogging keys, as required to service and adjust hardware items.

2.4 FASTENERS

Provide fasteners of type, quality, size, and quantity appropriate to the specific application. Fastener finish to match hardware. Provide stainless steel or nonferrous metal fasteners in locations exposed to weather. Verify metals in contact with one another are compatible and will avoid galvanic corrosion when exposed to weather.

2.5 FINISHES

Provide in accordance with [ANSI/BHMA A156.18](#). Provide hardware in BHMA 630 finish (satin stainless steel), unless specified otherwise. Provide items not manufactured in stainless steel in BHMA 626 finish (satin chromium plated) over brass or bronze, except aluminum paint finish for surface door closers, and except BHMA 652 finish (satin chromium plated) for steel hinges. Provide hinges for exterior doors in stainless steel with BHMA 630 finish. Furnish exit devices in BHMA 626 finish in lieu of BHMA 630 finish except where BHMA 630 is specified under paragraph HARDWARE SETS. Match exposed parts of concealed closers to lock and door trim. Match hardware finish for aluminum doors to the doors.

2.6 KEY CABINET AND CONTROL SYSTEM

Provide in accordance with [ANSI/BHMA A156.5](#), Type required to yield a capacity (number of hooks) 50 percent greater than the number of key changes used for door locks.

PART 3 EXECUTION

3.1 INSTALLATION

Provide hardware in accordance with manufacturers' printed installation instructions. Fasten hardware to wood surfaces with full-threaded wood screws or sheet metal screws. Provide machine screws set in expansion shields for fastening hardware to solid concrete and masonry surfaces. Provide toggle bolts where required for fastening to hollow core construction. Provide through bolts where necessary for satisfactory installation.

3.1.1 Weatherstripping Installation

Provide full contact, weathertight seals that allow operation of doors without binding the weatherstripping.

3.1.1.1 Stop Applied Weatherstripping

Fasten in place with color matched sheet metal screws not more than [9 inch](#) on center after doors and frames have been finish painted.

3.1.1.2 Interlocking Type Weatherstripping

Provide interlocking, self adjusting type on heads and jambs and flexible hook type at sills. Nail weatherstripping to door [1 inch](#) on center and to heads and jambs at [4 inch](#) on center.

3.1.1.3 Spring Tension Type Weatherstripping

Provide spring tension type on heads and jambs. Provide bronze nails with bronze. Provide stainless steel nails with stainless steel. Space nails not more than [1-1/2 inch](#) on center.

3.1.2 Soundproofing Installation

Provide as specified for stop applied weatherstripping.

3.1.3 Threshold Installation

Extend thresholds the full width of the opening and notch end for jamb stops. Set thresholds in a full bed of sealant and anchor to floor with cadmium-plated, countersunk, steel screws in expansion sleeves. For aluminum thresholds placed on top of concrete surfaces, coat the underside surfaces that are in contact with the concrete with fluid applied waterproofing as a separation measure prior to placement.

3.2 FIRE DOORS AND EXIT DOORS

Provide hardware in accordance with [NFPA 72](#) for door alarms, [NFPA 80](#) for fire doors, [NFPA 101](#) for exit doors, and [NFPA 252](#) for fire tests of door assemblies. .

3.3 HARDWARE LOCATIONS

Provide in accordance with [SDI/DOOR A250.8](#), unless indicated or specified otherwise.

- a. Kick and Armor Plates: Push side of single-acting doors. Both sides of double-acting doors.
- b. Mop Plates: Bottom flush with bottom of door.

3.4 KEY CABINET AND CONTROL SYSTEM

Locate where directed. Tag one set of file keys and one set of duplicate keys. Place other keys in appropriately marked envelopes, or tag each key. Provide complete instructions for setup and use of key control system. On tags and envelopes, indicate door and room numbers or master or grand master key.

3.5 FIELD QUALITY CONTROL

After installation, protect hardware from paint, stains, blemishes, and other damage until acceptance of work. Submit notice of testing 15 days before scheduled, so that testing can be witnessed by the Contracting Officer. Adjust hinges, locks, latches, bolts, holders, closers, and other items to operate properly. Demonstrate that permanent keys operate respective locks, and give keys to the Contracting Officer. Correct, repair, and finish, errors in cutting and fitting and damage to adjoining work.

3.6 HARDWARE SETS

DOOR HARDWARE SETS

The following hardware sets shall be provided and submitted for Government approval as required in Section 01 33 00 SUBMITTAL PROCEDURES and Section 08 71 00 DOOR HARDWARE.

Set: 1.0

Description: Exterior Pair Entry AL (CR)

Doors: 100A

2	Continuous Hinge (Alum)	A31331G	628
1	Removable Mullion	Type 22 - Keyed Removable	US28
1	Rim Exit Devise, Exit Only	Type 1 GR1 F01 x CD	US32D
1	Rim Exit Device, Nightlatch	Type 1 GR1 F01 x CD no trim	US32D
2	Cylinder	Best - Type as req'd for cyl.dogging	626
1	Cylinder	Best - Type as req'd for exit device	626
1	Cylinder	Best - Type as req'd for keyswitch	626
1	Cylinder	Best - Type as req'd for mullion	626
2	Door Pull	J402 1" x 12" x 45° offset pull HD mount	US32D
1	Concealed Overhead Stop	C01541	630
1	Door Closer PA	C02021 PT4H-BF/PT4D	AL
1	Drop Plate	As Required for Closer	AL
1	Blade Stop Spacer	As Required for Closer	AL
1	Automatic Operator	To Meet ANSI/BHMA A156.19	689
2	Sweep	R3B435	
1	Threshold	J35130	
1	Actuator - Wall mount	4-1/2" H x 4-1/2" W with Handicap Logo	US32D
1	Actuator - Frame mount	4-1/2" H x 1-11/16" W with Handicap Logo	US32D
1	Keyswitch	Single Gang Alternate Action	
1	Balanced Magnetic Switch	By Access Control; prep by D/F Mfr	
1	Card Reader	By Access Control	
1	Power Supply	By Access Control	

DOOR HARDWARE SETS

The following hardware sets shall be provided and submitted for Government approval as required in Section 01 33 00 SUBMITTAL PROCEDURES and Section 08 71 00 DOOR HARDWARE.

NOTES:

Perimeter seal and astragal by door supplier.

Operation:

- a. Doors electronically locked during established time zones as programmed by the access control system (fail secure function). When devices are locked, then the card reader grants access upon presentation of a valid credential. Exit devices mechanically lock during power failure with a mechanical key override for entry.
- b. Egress always free from inside by depressing inside exit device.
- c. Request to exit switch in the push pad to signal authorized egress and access control system.
- d. Balanced magnetic switch to signal door open/closed to the access control system.
- e. Inside and outside actuator switches for door operators are always active unless power to the operators is turned off.
- f. When doors are locked mechanically, then door operators are turned off using the wall mounted key switch.

Set: 2.0

Description: Exterior Pair Entry AL (CR)

Doors 101A, 101B

2	Continuous Hinge (Alum)	A31331G w/ PT	628
1	Removable Mullion	Type 22 - Keyed Removable	US28
1	Exit Device w/ ELR	Type 1 GR1 F03 E01 E04 x no trim	US32D
1	Rim Exit Device, EO / RX	Type 1 GR1 F01 E01 E04	US32D
1	Cylinder	Best - Type as req/d for exit device	626
1	Cylinder	Best - Type as req/d for mullion	626
2	Door Pull	J402 1" x 12" x 45° offset pull HD mount	US32D
2	Concealed Overhead Stop	C01541	630
2	Door Closer PA	C02021PT4H-BF/PT4D	AL
2	Drop Plate	As required for Closer	AL
2	Blade Stop Spacer	As required for Closer	AL
2	Sweep	R3B435	
1	Threshold	J35130	
2	Wire Harness	Wiring Harness W/ Plugin Connectors (Door)	
2	Wire Harness	Wiring Harness W/ Plugin Connectors (Frame)	

DOOR HARDWARE SETS

The following hardware sets shall be provided and submitted for Government approval as required in Section 01 33 00 SUBMITTAL PROCEDURES and Section 08 71 00 DOOR HARDWARE.

- 2 Balanced Magnetic Switch By Access Control; Prep by D/F Mfr.
- 1 Power Supply By Access Control

NOTES:

- a. Doors electronically locked during established time zones as programmed by the access control system (fail secure function). Exit devices mechanically lock during power failure with a mechanical key override for entry.
- b. Egress always free from inside by depressing inside exit device.
- c. Request to exit switch in lever to signal authorized egress to the access control system.
- d. Balanced magnetic switch to signal door open/closed to the access control system.

Set: 3.0

Description: Exterior Single COMM, Paint/Comm Rated (CR)

Doors 116

3	Hinges, Hvy Wt	A8111 4 1/2" x 4 1/2" NRP	US32D
1	Mortise Lock (storeroom)	1000 Grade 1 F07 Lever	626
1	Cylinder	Best - Type as req'd for lock	626
1	Door Closer w/stop	C02021 PT4H-BR/PT4D/PT4G	AL
1	Kick Plate	J102 10" x 2" LDW BEV CSK	US32D
1	Gasketing	R3E165 (Head & Jamb)	
1	Rain Guard	RAY976	
1	Sweep	R3B435	
1	Threshold	J35130	

Set: 4.0

Description: Exterior Single Wash Equipment - Exit Only (Monitor)

Doors 121B

3	Hinges, Hvy Wt	A8111 4 1/2" x 4 1/2" NRP	US32D
1	Rim Exit Device, Exit Only	Type 1 GR 1 F09 Lever	US32D
1	Cylinder	Best - Type as req'd for lock	626
1	Door Closer w/stop	C02021 PT4H-BR/PT4D/PT4G	AL

DOOR HARDWARE SETS

The following hardware sets shall be provided and submitted for Government approval as required in Section 01 33 00 SUBMITTAL PROCEDURES and Section 08 71 00 DOOR HARDWARE.

1	Kick Plate	J102 10" x 2" LDW BEV CSK	US32D
1	Gasketing	R3E165 (Head & Jamb)	
1	Rain Guard	RAY976	
1	Sweep	R3B435	
1	Threshold	J35130	

Set: 5.0

Description: Exterior Single Mechanical (Monitor)

Doors 122B, 122C

3	Hinges, Hvy Wt	A8111 4 1/2" x 4 1/2" NRP	US32D
1	Mortise Lock (storeroom)	1000 Grade 1 F07 Lever	626
1	Cylinder	Best - Type as req'd for lock	626
1	Door Closer w/stop	C02021 PT4H-BR/PT4D/PT4G	AL
1	Kick Plate	J102 10" x 2" LDW BEV CSK	US32D
1	Gasketing	R3E165 (Head & Jamb)	
1	Rain Guard	RAY976	
1	Sweep	R3B435	
1	Threshold	J35130	

Set: 6.0

Description: Exterior Single Hangar Bay

Doors 106B, 113B, 120B

3	Hinges, Hvy Wt	A8111 4 1/2" x 4 1/2" NRP	US32D
1	Rim Exit Device, Exit only	Type 1GR1 F01	US32D
1	Door Closer PA	C02021 PT4h-bf/pt4d	AL
1	Kick Plate	J102 10" x 2" LDW BEV CSK	US32D
1	Wall Stop	L02251	US32D
1	Gasketing	R3E165 (Head & Jamb)	
1	Rain Guard	RAY976	
1	Sweep	R3B435	

DOOR HARDWARE SETS

The following hardware sets shall be provided and submitted for Government approval as required in Section 01 33 00 SUBMITTAL PROCEDURES and Section 08 71 00 DOOR HARDWARE.

1 Threshold J35130

Set: 7.0

Description: Exterior Pair Fire Pump Room, Exterior Pair Mechanical

Doors 102,105

6	Hinges	A8111 4 1/2" x 4 1/2" NRP	US32D
2	Manual Flush Bolt	L04251	US26D
1	Dust Proof Stike	L04021 w/floor plate	US26D
1	Mortise Lock (storeroom)	1000 Grade 1 F07 Lever x 7/8" Lip	626
1	Cylinder	Type as req'd for lock	626
2	Door Closer w/stop	C02021 PT4H-BF/PT4D/PT4G	AL
2	Kick Plate	J102 10" x 2" LDW BEV CSK	US32D
1	Overlapping Astragal	ROY636	
1	Gasketing	ROY165 (Head & Jamb)	
1	Rain Guard	ROY906	
2	Sweep	ROY536	
1	Threshold	J35130	

Set: 8.0

Description: Exterior Pair Electrical

Doors 104, 123

6	Hinges, Hvy Wt	A8111 4 1/2" x 4 1/2" NRP	US32D
1	Removable Mullion	Type 22 - Keyed removable	US28
1	Rim Exit Device, Exit Only	Type1 GR1 F01	US32D
1	Rim exit Device, Storeroom	Type 1 GR1 F03 Lever	US32D
1	Cylinder	Type as req'd for exit device	626
1	Cylinder	Type as req'd for mullion	626
2	Door Closer w/stop	C02021 PT4H-BF/PT4D/T4G	AL
2	Kick Plate	J102 10" x 2" LDW BEV CSK	US32D
1	Gasketing, Mullion	R0C004	

DOOR HARDWARE SETS

The following hardware sets shall be provided and submitted for Government approval as required in Section 01 33 00 SUBMITTAL PROCEDURES and Section 08 71 00 DOOR HARDWARE.

1	Gasketing	ROY165 (Head & Jamb)
1	Rain Guard	ROY906
2	Sweep	ROY536
1	Threshold	J35130

Set: 9.0

Description: Interior Pair Wash Equipment(FR)

Door: 121A

6	Hinge, Hvy Wt	A8111 4-1/2" x 4-1/2"	US32D
1	Dust Proof Strike	L04021 w/floor plate	US26D
1	Auto Flush Bolt	Type 25 (set)	US26D
1	Mortise Lock (classroom)	1000 Grade 1 F05 Lever	626
1	Cylinder	Type as req'd for lock	626
1	Coordinator	Type 21A	Black
2	Surface Overhead Stop	C02541	630
2	Door Closer Reg	C02011 PT4H-BF/PT4D	AL
2	Kick Plate	J102 10" x 2" LDW BEV CSK	US32D
1	Overlapping Astragal	ROY 636	
2	Automatic Door Bottom	Semi-mortised	Powder coat to match door color
1	Gasketing	ROE154	
1	Gasketing	ROE154 Mounted to astragal	
1	Threshold	JE2100	

Notes: Mount astragal on pull side of inactive leaf and size doors for 1/8" clearance between leaves. Paint astragal to match doors.

Set: 10.0

Description: Interior Pair Entry Vestibule (AL)

Doors 100B

2	Continuous Hinge (Alum)	A31331G w/ PT	628
2	Door Pull	J402 1" x 12" x 45 offset pull HD mount	US32D

DOOR HARDWARE SETS

The following hardware sets shall be provided and submitted for Government approval as required in Section 01 33 00 SUBMITTAL PROCEDURES and Section 08 71 00 DOOR HARDWARE.

2	Dummy Touchbar	H673DR	630
1	Concealed Overhead Stop	C01541	630
1	Door Closer PA	C02021 PT4H-BF/PT4D	AL
1	Drop Plate	As required for Closer	AL
1	Blade Stop Spacer	As required for Closer	AL
1	Automatic Operator	To meet ANSI/BHMA A156.19	689
1	Actuator - Frame mount	4 1/2"H x 1 11/16"W with Handicap Logo	US32D
1	Actuator - Wall mount	4 1/2"H x 4 1/2"W with Handicap Logo	US32D

Set: 11.0

Description: Interior - Single Catwalk

Doors 106C, 113C

3	Hinges, Hvy Wt	A8111 4 1/2" x 4 1/2" NRP	US32D
1	Passage Latchset-Lever		630
1	Door Closer w/stop	C02021 PT4H-BF/PT4D/T4G	AL
1	Kick Plate	J102 10" x 2" LDW BEV CSK	US32D
1	Wall Stop, Convex	L02101	US26D
3	Silencer	Metal frame type	

Set: 12.0

Description: Interior Single RVE Storage (FR)

Doors 109A

3	Hinges, Hvy Wt	A8111 4 1/2" x 4 1/2" NRP	US32D
1	Mortise Lock (storeroom)	1000 Grade 1 F07 Lever x 7/8" Lip	626
1	Cylinder	Type as req'd for lock	626
1	Door Closer w/stop	C02021 PT4H-BF/PT4D/T4G	AL
1	Kick Plate	J102 10" x 2" LDW BEV CSK	US32D
1	Wall Stop, Convex	L02101	US26D
3	Silencer	Metal frame type	
1	Smoke Gasketing	ROE154	

DOOR HARDWARE SETS

The following hardware sets shall be provided and submitted for Government approval as required in Section 01 33 00 SUBMITTAL PROCEDURES and Section 08 71 00 DOOR HARDWARE.

Set: 13.0

Description: Interior Single RVE Storage - Exit only

Doors 109B

3	Hinges, Hvy Wt	A8111 4 1/2" x 4 1/2" NRP	US32D
1	Mortise Lock (storeroom)	1000 Grade 1 F07 Lever x 7/8" Lip	626
1	Cylinder	Type as req'd for lock	626
1	Door Closer, reg	C02011 PT4H-BF/PT4D	AL
1	Kick Plate	J102 10" x 2" LDW BEV CSK	US32D
1	Wall Stop, Convex	L02101	US26D
3	Silencer	Metal frame type	
1	Smoke Gasketing	ROE154	

Set: 14.0

Description: Interior Single Mother's (STC)

Door: 110A

3	Hinges, Hvy Wt	A8111 4-1/2" x 4-1/2"	US26D
1	Mortise Lock (privacy)	1000 Grade I F02 Lever VIN	626
1	Cylinder	Type as req'd for lock	626
1	Door Closer PA	C02021 PT4H-BF/PT4D	AL
1	Kick Plate	J102 10" x 2" LDW BEV CSK	US26D
3	Silencer	Metal Frame type	

Note:

Hinges, perimeter seals, door bottom and threshold (if required) provided by acoustic door manufacturer to meet STC and ABA opening requirements.

Set: 15.0

Description: Interior Single Office(STC)

Door: 111

3	Hinges, Hvy Wt	A8111 4-1/2" x 4-1/2" NRP	US26D
1	Mortise Lock (entry)	1000 Grade I F04 Lever	626
1	Cylinder	Type as req'd for lock	626

DOOR HARDWARE SETS

The following hardware sets shall be provided and submitted for Government approval as required in Section 01 33 00 SUBMITTAL PROCEDURES and Section 08 71 00 DOOR HARDWARE.

1	Door Closer	C02021 PT4H-BF/PT4D	AL
1	Kick Plate	J102 10"x2" LDW BEV CSK	US32D
3	Silencer	Metal Frame type	

Note:

Hinges, perimeter seals, door bottom and threshold (if required) provided by acoustic door manufacturer to meet STC and ABA opening requirements.

Set: 16.0

Description: Interior Single Electrical

Door: 115

3	Hinges, Hvy Wt	A8111 4-1/2" x 4-1/2" NRP	US26D
1	Rim Exit Device, Storeroom	Type 1 GR1 F09 Lever	US32D
1	Cylinder	Type as req'd for lock	626
1	Door Closer w/Stop	C02021 PT4H-BF/PT4D/PT4G	AL
1	Kick Plate	J102 10"x2" LDW BEV CSK	US32D
1	Wall Stop, Convex	L0201	US26D

Set: 17.0

Description: Interior Single Restrooms(STC)

Doors: 117, 118

3	Hinge, Hvy Wt	A8111 4-1/2" x 4-1/2" NRP	US26D
1	Push Plate	J301 8" x 16" .050	US32D
1	Pull Plate	J405 1" x 10" pull, 4" x 16" plate, .050	US32D
1	Door Closer Reg	C02011 PT4H-BF/PT4D	AL
1	Kick Plate	J102 10" x 2" LDW BEV CSK	US32D
1	Floor Stop	L02161	US26D
3	Silencer	Metal frame type	

Set: 18.0

Description: Interior Pair Tool RM/ALIS - 180 Swing

Door: 103A (tool)

3	Hinge, Hvy Wt	A8121 4-1/2" x 4-1/2" NRP	US32D
---	---------------	---------------------------	-------

DOOR HARDWARE SETS

The following hardware sets shall be provided and submitted for Government approval as required in Section 01 33 00 SUBMITTAL PROCEDURES and Section 08 71 00 DOOR HARDWARE.

3	Hinge, Hvy Wt	A8121 4-1/2" x 4-1/2" NRP; 180°	US32D
1	Dust proof Strike	L04021 w/floor plate	US26D
1	Auto Flush Bolt	Type 25 (set)	US26D
1	Mortise Lock (classroom)	1000 Grade 1 F05 Lever	626
1	Cylinder	Type as Req'd for Lock	626
1	Coordinator	Type 21A	Black
2	Door Closer w/stop	C02021 PT4H-BF/PT4D/PT4G	AL
2	Kick Plate	J102 10" x 2" LDW BEV CSK	US32D

Set: 19.0

Description: Interior Pair Vestibule

Doors: 107A, 112A, 119A

6	Hinge, Hvy Wt	A8111 4-1/2" x 4-1/2" NRP	US26D
2	Dummy Touchbar	N673DR	US32D
2	Pull Plate	J405 1" x 10" Pull, 4" x 16" Plate, .050	US32D
2	Kick Plate	J102 10" x 2" LDQ BEV CSK	US32D
2	Door Closer Reg	C02011 PT4H-BF/PT4D	AL
2	Silencer	Metal frame type	

Notes:

Operation:

1. Magnetic hold opens to release upon fire alarm or power failure.

Set: 20.0

Description: Interior Pair Vestibule(FR)(CR)

Doors: 107B, 112B, 119B (VEST)

6	Hinge, Hvy Wt	A8111 4-1/2" x 4-1/2" NRP	US26D
AM0003* 1	<u>Surface Vertical Rod Exit Device, Non-Electrified, Exit Only, LHR</u> ~~Rim Exit Device, Exit Only~~	Type 1 GR1 F01	US32D

*AM0003

DOOR HARDWARE SETS

The following hardware sets shall be provided and submitted for Government approval as required in Section 01 33 00 SUBMITTAL PROCEDURES and Section 08 71 00 DOOR HARDWARE.

AM0003*	1	<u>Surface Vertical Rod Exit Device, Electrified, RHR</u> ~~Rim Exit Device,~~ (Classroom)	Type 1GR1 ~~F0308~~ Lever	US32D	
	1	Cylinder	Type as Req'd for exit device	626	
	4	~~Automatic Flush Bolt~~	~~Type 25, Set~~	~~US26D~~	
	2	Door Closer PA	C02021 PT4H-BF/PT4D	AL	
	~~42~~	~~Dustproof Top~~ Strike	~~646L04021 w/ Floor Plate~~	US26D	
	2	<u>Bottom Strike</u>	<u>655</u>	<u>US26D</u>	
	2	Kick Plate	J102 10" x 2" LDQ BEV CSK	US32D	
	4	~~Coordinator~~	~~Type 21A~~	~~Black~~	*AM0003
	2	Floor Stop	L02161	US26D	
	1	Wire Harness	Wireing Harness W/ Plugin Connectors (Door)		
	1	Wire Harness	Wireing Harness W/ Plugin Connectors (Frame)		
	1	Balanced Magnetic Switch	By Access Control; Prep by D/F Mfr.		
	1	Card Reader	By Access Control		
	1	Power Supply	By Access Control		

Operation:

- Doors electrically unlocked or locked during established time zones as programmed by the access control system. When outside lever is locked the card reader grants access upon presentation of a valid credential. Locksets mechanically lock during power failure with a mechanical key override entry.
- Egress always free from hangar side by depressing inside lever.
- Request to exit switch in lever to signal authorized egress to the access control system.
- Balanced magnetic switch to signal door open/closed to the access control system.

Set: 21.0

Description: Interior Pair Janitor

Door: 108

6	Hinge, Hvy Wt	A8111 4-1/2" x 4-1/2" NRP	US26D
1	Mortise Lock (storeroom)	1000 Grade 1 F05 Lever	626
2	Cylinder	Type as req'd for lock	626

DOOR HARDWARE SETS

The following hardware sets shall be provided and submitted for Government approval as required in Section 01 33 00 SUBMITTAL PROCEDURES and Section 08 71 00 DOOR HARDWARE.

2	Door Closer w/stop	C02021 PT4H-BF/PT4D/PT4G	AL
2	Kick Plate	J102 10" x 2" LDW BEV CSK	US32D
6	Silencer	Metal frame type	

-- End of Section --

SECTION TABLE OF CONTENTS

DIVISION 09 - FINISHES

SECTION 09 06 00

SCHEDULES FOR FINISHES

PART 1 GENERAL

- 1.1 SUMMARY
- 1.2 SUBMITTALS
- 1.3 COLOR REFERENCE SYSTEMS

PART 2 PRODUCTS

- 2.1 CONTRACTOR COLOR BOARDS
- 2.2 COLOR SCHEDULE
- 2.3 EXTERIOR FINISHES
 - 2.3.1 Exterior Walls
 - 2.3.1.1 Brick
 - 2.3.1.2 Metal Wall Panels, Hardware, and Associated Trim
 - 2.3.1.3 Glass and Glazing
 - 2.3.2 Exterior Trim
 - 2.3.2.1 Steel Doors and Door Frames
 - 2.3.2.2 Aluminum Doors and Door Frames
 - 2.3.2.3 Aluminum Windows (mullion, muntin, sash, trim, and sill)
 - 2.3.2.4 Fascia
 - 2.3.2.5 Soffits
 - 2.3.2.6 Downspouts and Gutters
 - 2.3.2.7 Louvers
 - 2.3.2.8 Flashings
 - 2.3.2.9 Cast Stone Caps, Water Tables and Sills
 - 2.3.2.10 Caulking and Sealants
 - 2.3.2.11 Bollards
 - 2.3.2.12 Signage
 - 2.3.2.13 Control Joints
 - 2.3.2.14 Expansion Joint and/or Covers
 - 2.3.3 Exterior Roof
 - 2.3.3.1 Metal
 - 2.3.3.2 Penetrations
- 2.4 INTERIOR FINISHES
 - 2.4.1 Interior Floor Finishes
 - 2.4.1.1 Aluminum Transition
 - 2.4.1.2 Entrance Mat
 - 2.4.1.3 Plastic Laminate
 - 2.4.1.4 Concrete (Sealed Hardener-Densifier)
 - 2.4.1.5 Industrial Floor Coating
 - 2.4.2 Interior Base Finishes
 - 2.4.2.1 Resilient Base and Moldings
 - 2.4.2.2 Integral Cove Base
 - 2.4.3 Interior Wall Finishes
 - 2.4.3.1 Paint
 - 2.4.3.2 Ceramic Tile

- 2.4.3.3 Grout
- 2.4.3.4 Metal Liner Panels
- *AM0003 2.4.3.5 Exposed Structural Columns AM0003*
- 2.4.4 Interior Ceiling Finishes
 - 2.4.4.1 Acoustical Tile and Grid
 - 2.4.4.2 Paint (Ceilings)
 - 2.4.4.3 Metal Deck
 - 2.4.4.4 Structural Framing
- 2.4.5 Interior Trim
 - 2.4.5.1 Steel Doors
 - 2.4.5.2 Steel Door Frames
 - 2.4.5.3 Aluminum Doors and Door Frames
 - 2.4.5.4 Aluminum Windows (mullion, muntin, sash, trim, and stool)
 - 2.4.5.5 Wood Doors
 - 2.4.5.6 Wood Stain
 - 2.4.5.7 Fire Extinguisher Cabinets
 - 2.4.5.8 Guardrails
 - 2.4.5.9 Ladders
 - 2.4.5.10 Exposed Ductwork
- 2.4.6 Interior Miscellaneous
 - 2.4.6.1 Toilet Partitions and Urinal Screens
 - 2.4.6.2 Casework
 - 2.4.6.3 Plastic Laminate
 - 2.4.6.4 Solid Surfacing Material
 - 2.4.6.5 Window Sills (Solid Surface)
 - 2.4.6.6 Corner Guards
 - 2.4.6.7 Signage Message Color
 - 2.4.6.8 Signage Background Color
 - 2.4.6.9 Building Directory
 - 2.4.6.10 Bulletin Board
 - 2.4.6.11 Lockers
 - 2.4.6.12 Benches
 - 2.4.6.13 Wall Switch Handles and Standard Receptacle Bodies
 - 2.4.6.14 Electrical Device Cover Plates
 - 2.4.6.15 Electrical Panels
 - 2.4.6.16 Shower Curtain
 - 2.4.6.17 Shower Wall Kits, Trim and Shower Pan

PART 3 EXECUTION

-- End of Section Table of Contents --

SECTION 09 06 00
SCHEDULES FOR FINISHES

PART 1 GENERAL

1.1 SUMMARY

This section covers only the color of exterior and interior materials and products that are exposed to view in the finished construction. The word "color", as used herein, includes surface color and pattern. Requirements for quality, product specifications, and method of installation are covered in other appropriate sections of the specifications. Specific locations where the various materials are required are shown on the drawings if not identified in this specification. Items not designated for color in this section may be specified in other sections. When color is not designated for items, propose a color for approval.

1.2 SUBMITTALS

Government approval is required for submittals with a "G" or "S" classification. Submittals not having a "G" or "S" classification are for information only. When used, a code following the "G" classification identifies the office that will review the submittal for the Government. Submit the following in accordance with Section 01 33 00 SUBMITTAL PROCEDURES.

Products listed by manufacturer are for identification and performance purposes only. They are not intended to limit selection from other manufacturers. However, colors, patterns textures and profiles must match those listed in legend in order to maintain color coordination and visual design integrity.

SD-04 Samples

Contractor Color Boards; G

1.3 COLOR REFERENCE SYSTEMS

Colors for project finishes are identified in the Color Schedule and based on the RGB (Red, Green and Blue) color reference system.

PART 2 PRODUCTS

2.1 CONTRACTOR COLOR BOARDS

Contractor to submit actual color boards to include all finish color samples specified on the project, prior to the submittal and approval of individual finish submittals. The DOR must review and approve the color boards to verify overall building finish coordination and aesthetic. Color boards must be prepared by professional interior designers or architects with significant interior design experience. Qualification of designers is based on education, experience and examination. Interior designers or architects must have completed a program accredited by the Council for Interior Design Accreditation (CIDA) or equal accreditation program of academic training in interior design. In addition, the interior designer or architect must also have attained National Council for Interior Design Qualification (NCIDQ) certification or state licensure, certification or registration and must not be affiliated with a furniture dealership, vendor or manufacturer.

2.2 COLOR SCHEDULE

The color information provided in the following paragraphs lists the colors, patterns and textures for exterior and interior finishes, including both factory applied and field applied colors. In the case of difference between the drawings and specifications, colors identified in this specification govern.

2.3 EXTERIOR FINISHES

Reference drawings for color information.

2.3.1 Exterior Walls

Exterior wall colors apply to exterior wall surfaces including recesses at entrances and projecting vestibules. When applicable, paint conduit to closely match the adjacent surface color. Provide wall colors to match the colors listed below.

2.3.1.1 Brick

Basis of Design: Acme Brick, 2001 Old Greenwood Rd., Fort Smith, AR 72903.

"Flying Razorback Blend"

Color 1 - Napa Valley

Color 2 - Garnet

Color 3 - Crimson

2.3.1.2 Metal Wall Panels, Hardware, and Associated Trim

Basis of Design: Metl-Span, a Nucor Company, 700 State Highway 121 Bypass, Suite 200, Lewisville, TX 75067

Color - "Dove Tail" or equal

2.3.1.3 Glass and Glazing

Basis of Design: Color - Clear

2.3.2 Exterior Trim

Provide exterior trim to match the colors listed below.

2.3.2.1 Steel Doors and Door Frames

Basis of Design:

At full brick: Color - to match metal roof, "Dark Bronze" HEX# 534842 or equal

At Metal Panel and brick wainscot: Color - to match metal panel, "Dove Tail" or equal

2.3.2.2 Aluminum Doors and Door Frames

Color: Anodized Aluminum - Clear

2.3.2.3 Aluminum Windows (mullion, muntin, sash, trim, and sill)

Color: Anodized Aluminum - Clear

2.3.2.4 Fascia

Basis of Design: Color - to match "Dark Bronze" HEX# 534842 or equal

2.3.2.5 Soffits

Metal Panel soffit to match walls: Color "Dove Tail" or equal

2.3.2.6 Downspouts and Gutters

Basis of Design:

At full brick: Color - to match metal roof, "Dark Bronze" HEX# 534842 or equal

At Metal Panel and brick wainscot: Color - to match metal panel, "Dove Tail" or equal

2.3.2.7 Louvers

Basis of Design: Color - to match "Dove Tail" or equal

2.3.2.8 Flashings

Match adjacent material in color.

2.3.2.9 Cast Stone Caps, Water Tables and Sills

Basis of Design: DFW Cast Stone, 2416 Weaver St., Haltom City, TX 76117

Color - Dark Buff by DFW Cast Stone or Equal

2.3.2.10 Caulking and Sealants

Match adjacent material in color.

2.3.2.11 Bollards

Color: Safety Yellow

2.3.2.12 Signage

Refer to drawings

2.3.2.13 Control Joints

Match adjacent material in color.

2.3.2.14 Expansion Joint and/or Covers

Match adjacent material in color.

2.3.3 Exterior Roof

Apply roof color to exterior roof surfaces including sheet metal flashings and copings, snow guards, mechanical units, mechanical penthouses, roof trim, pipes, conduits, electrical appurtenances, and similar items. Provide roof color to match the colors listed below.

2.3.3.1 Metal

Basis of Design: Color - FED-STD-595C 30040 "Dark Bronze" HEX# 534842 or equal

2.3.3.2 Penetrations

Match roof in color.

2.4 INTERIOR FINISHES

2.4.1 Interior Floor Finishes

Provide flooring materials to match the colors listed below.

2.4.1.1 Aluminum Transition

Clear Anodized

2.4.1.2 Entrance Mat

WOM-1: Shaw Contract, Stepping out 5T031 - Sterling 31557

2.4.1.3 Plastic Laminate

Wilsonart: Phantom Cocoa, 8213K-28

2.4.1.4 Concrete (Sealed Hardener-Densifier)

PC-1: Matte, slip resistance 0.65 COF or greater

2.4.1.5 Industrial Floor Coating

RES-1: Stonhard, Stonetec UTF, TEC4-63B, Large Flakes

RES-2: Stonchem, Stonechem X58/X5HD - 5 Coat, color/pattern to match Stonechem UTF, TEC4-63B, Large Flakes

RES-3: Stonchem, Stonechem X58/X5HD - 5 Coat - White

RES-4: Stonchem, Stonechem X58/X5HD - 5 Coat Floor Marking - Yellow

RES-5: Stonchem, Stonechem X58/X5HD - 5 Coat Floor Marking - Red

RES-6: Stonchem, Stonechem X58/X5HD - 5 Coat Floor Marking - Green

2.4.2 Interior Base Finishes

Provide base materials to match the colors listed below.

2.4.2.1 Resilient Base and Moldings

RB-1: Tarkett Baseworks: 38 Pewter

2.4.2.2 Integral Cove Base

RESB-1: Stonehard and Stonechem to match Res-1, Res-2, Res-3

2.4.3 Interior Wall Finishes

Apply interior wall color to the entire wall surface, including reveals, vertical furred spaces and columns, grilles, diffusers, electrical and access panels, and piping and conduit adjacent to wall surfaces unless otherwise specified. Paint items not specified in other paragraphs to match adjacent wall surface. Provide wall materials to match the colors listed below.

2.4.3.1 Paint

Epoxy and Laytex: PT-1, PT-2, PT-3 Field: Color: Benjamin Moore - OC-130 Cloud White

Epoxy and Laytex: PT-4, PT-5 Ceiling: Color: Sherwin Williams - SW7005 Pure White

Epoxy and Laytex: PT-7 Accent: Color: Sherwin Williams - SW6524 Commodore

Epoxy: PT-6, PT-8 Field: Sherwin Williams - SW7075 Web Gray

For structural steel paint refer to spec section 09 97 13.27

2.4.3.2 Ceramic Tile

TLC-1: Marazzi - MT12 Off White

TLC-2: Daltile - Color Wheel Classic- 1174 Sea Breeze Gloss

TLC-3: Daltile - - Color Wheel Classic1469 Galazy Gloss

2.4.3.3 Grout

GR-2: Mapei, 93 Warm Grey

2.4.3.4 Metal Liner Panels

Color to match Benjamin Moore - OC-130 Cloud White

*AM0003 2.4.3.5 Exposed Structural Columns

Refer to spec section 09 97 13.27. Color to be white. Epoxy: PT-2 Field: Color: Benjamin Moore - OC-130 Cloud White

AM0003*

2.4.4 Interior Ceiling Finishes

Apply ceiling colors to ceiling surfaces including soffits, furred down areas, grilles, diffusers, registers, and access panels. In addition, apply ceiling color to joists, underside of roof deck, and conduit and piping where joists and deck are exposed and required to be painted. Provide ceiling materials to match the colors listed below.

2.4.4.1 Acoustical Tile and Grid

ACT-1: ARMSTRONG CEILINGS - Ultima Beveled Tegular - 1941, White, Prelude White
15/16" Grid

2.4.4.2 Paint (Ceilings)

In Restrooms: Epoxy
PT-2: Benjamin Moore - OC-130 Cloud White
In Mother's Room: Laytex
PT-1: Benjamin Moore - OC-130 Cloud White

2.4.4.3 Metal Deck

In Hangars, RVE Storage and Wash Bays: Epoxy
PT-2: Benjamin Moore - OC 130 Cloud White
In all other Open to structure rooms: Epoxy
PT-6: Sherwin Williams - SW7075 Web Gray

2.4.4.4 Structural Framing

Epoxy
PT-1: Benjamin Moore - OC-130 Cloud White

2.4.5 Interior Trim

Provide interior trim to match the colors listed below.

2.4.5.1 Steel Doors

PT-6: Sherwin Williams - SW7075 Web Gray

2.4.5.2 Steel Door Frames

PT-6: Sherwin Williams - SW7075 Web Gray

2.4.5.3 Aluminum Doors and Door Frames

Prefinished Aluminum: Color - Anodized Aluminum, Clear

2.4.5.4 Aluminum Windows (mullion, muntin, sash, trim, and stool)

Prefinished Aluminum: Color - Anodized Aluminum, Clear

2.4.5.5 Wood Doors

Color to match Wilsonart 8213K-28 Phantom Cocoa

2.4.5.6 Wood Stain

Natural, clear

2.4.5.7 Fire Extinguisher Cabinets

Clear Anodized Aluminum

2.4.5.8 Guardrails

PT-6: Sherwin Williams - SW7075 Web Gray

2.4.5.9 Ladders

PT-6: Sherwin Williams - SW7075 Web Gray

2.4.5.10 Exposed Ductwork

PT-6: Sherwin Williams - SW7075 Web Gray

2.4.6 Interior Miscellaneous

Provide miscellaneous items to match the colors listed below.

2.4.6.1 Toilet Partitions and Urinal Screens

TP-1: Scranton Products - Eclipse Partitions - "Blueberry"

2.4.6.2 Casework

PLAM-1: Wilsonart 8213K-28 - Phantom Cocoa
SSF-1: Formica - 758 Blanco Mineral (Mother's Room)

2.4.6.3 Plastic Laminate

PLAM-1: Wilsonart 8213K-28 - Phantom Cocoa

2.4.6.4 Solid Surfacing Material

SSF-1: Formica - 758 Blanco Mineral
SSF-2: Formica - 757 Luna Sand

2.4.6.5 Window Sills (Solid Surface)

SSF-1: Formica - 758 Blanco Mineral

2.4.6.6 Corner Guards

CG-1: Construction Specialties - CO-8

2.4.6.7 Signage Message Color

To Match: PT-6: Sherwin Williams - SW7075 Web Gray

2.4.6.8 Signage Background Color

To Match: PT-1: Benjamin Moore - OC-130 Cloud White

2.4.6.9 Building Directory

To Match: PT-1: Benjamin Moore - OC-130 Cloud White

2.4.6.10 Bulletin Board

Cork: Natural Cork Tackable Panels - 24"w X 36"h x 2"d

2.4.6.11 Lockers

Manufacturer's Standard - grey

2.4.6.12 Benches

Manufacturer's Standard

2.4.6.13 Wall Switch Handles and Standard Receptacle Bodies

Manufacturer's Standard Grey

2.4.6.14 Electrical Device Cover Plates

Stainless Steel

2.4.6.15 Electrical Panels

Manufacturer's Standard Grey

2.4.6.16 Shower Curtain

Manufacturer's Standard

2.4.6.17 Shower Wall Kits, Trim and Shower Pan

SSF-2: Formica - Luna Sand

PART 3 EXECUTION

Not Used

-- End of Section --

SECTION TABLE OF CONTENTS

DIVISION 09 - FINISHES

SECTION 09 97 13.27

HIGH PERFORMANCE COATING FOR STEEL STRUCTURES

PART 1 GENERAL

- *AM0003 1.1 REFERENCES AM0003*
- 1.2 DEFINITIONS
- *AM0003 1.3 SUBMITTALS AM0003*
- 1.4 QUALITY ASSURANCE
 - 1.4.1 Contract Errors, Omissions, and Other Discrepancies
 - 1.4.2 Corrective Action (CA)
 - 1.4.2.1 Corrective Action Procedures
 - 1.4.2.2 Implement Corrective Action
 - 1.4.3 Coating Work Plan
 - 1.4.4 Design Data
 - 1.4.4.1 Containment System
 - 1.4.5 Test Reports
 - 1.4.5.1 Joint Sealant Qualification Test Reports
 - 1.4.5.2 Coatings Qualification Test Reports
 - 1.4.5.3 Metallic Abrasive Qualification Test Reports
 - 1.4.5.4 Recycled Metallic Abrasive Field Test Reports (Daily and Weekly)
 - 1.4.6 Qualifications
 - 1.4.6.1 Qualifications of Certified Industrial Hygienist (CIH)
 - 1.4.6.2 Qualifications of Certified Protective Coatings Specialist (PCS)
 - 1.4.6.3 Qualifications of Coating Inspection Company
 - 1.4.6.4 Qualifications of QC Specialist Coating Inspector
 - 1.4.6.5 Qualifications Of Individuals Performing Abrasive Blasting
 - 1.4.6.6 Qualifications of Testing Laboratory for Coatings
 - 1.4.6.7 Qualifications of Testing Laboratory for Abrasive
 - *AM0003 1.4.6.8 Qualifications of Coating Contractors AM0003*
 - 1.4.6.9 Joint Sealant Materials
 - 1.4.6.10 Coating Materials
 - 1.4.6.11 Coating System Component Compatibility
 - 1.4.6.12 Non-metallic Abrasive
 - 1.4.6.13 Metallic Abrasive
 - 1.4.7 Protective Coating Specialist (PCS)
 - 1.4.8 Pre-Application Meeting
- 1.5 PRODUCT DATA
 - 1.5.1 Joint Sealant Instructions
 - 1.5.2 Coating System Instructions
- 1.6 DELIVERY AND STORAGE
- 1.7 COATING HAZARDS
- *AM0003 1.8 JOB SITE REFERENCES AM0003*

PART 2 PRODUCTS

- 2.1 JOINT SEALANT
- 2.2 COATING SYSTEM
 - 2.2.1 Zinc-Rich Epoxy Primer Coat

- 2.2.2 Epoxy Intermediate Coat
- 2.2.3 Polyurethane Topcoat
- 2.3 COATING SAMPLE COLLECTION AND SHIPPING KIT
- 2.4 ABRASIVE SAMPLE COLLECTION AND SHIPPING KIT
- 2.5 TEST KITS
 - 2.5.1 Test Kit for Measuring Chloride, Sulfate and Nitrate Ions on Steel and Coated Surfaces
 - 2.5.2 Test Kit for Identifying Amine Blush on Epoxy Surfaces
- 2.6 ABRASIVE
 - 2.6.1 Non-metallic Abrasive
 - 2.6.2 Metallic Abrasive
 - 2.6.2.1 New and Remanufactured Steel Grit
 - 2.6.2.2 Recycled Steel Grit
- 2.7 WHITE ALUMINUM OXIDE NON-SKID GRIT

PART 3 EXECUTION

- 3.1 COATING AND ABRASIVE SAMPLE COLLECTION AND TESTING
 - 3.1.1 Coating Sample Collection
 - 3.1.2 Abrasive Sample Collection
 - 3.1.3 Coating Sample Test Reports
 - 3.1.4 Abrasive Sample Test Reports
- 3.2 SURFACES TO BE COATED
- 3.3 LIGHTING
- 3.4 ENVIRONMENTAL CONDITIONS
 - 3.4.1 Containment
 - 3.4.2 Automated Monitoring Requirements
- 3.5 SURFACE PREPARATION
 - 3.5.1 Abrasive Blasting Equipment
 - 3.5.2 Operational Evaluation of Abrasive
 - 3.5.3 Surface Standard
 - 3.5.4 Pre-Preparation Testing for Surface Contamination
 - 3.5.4.1 Pre-Preparation Testing for Oil and Grease Contamination
 - 3.5.4.2 Pre-Preparation Testing for Soluble Salts Contamination
 - 3.5.5 Abrasive Blasting
 - 3.5.6 Disposal of Used Abrasive
 - 3.5.7 Pre-Application Testing For Surface Contamination
 - 3.5.7.1 Pre-Application Testing for Oil and Grease Contamination
 - 3.5.7.2 Pre-Application Testing for Soluble Salts Contamination
 - 3.5.7.3 Pre-Application Testing for Surface Cleanliness
- 3.6 MIXING AND APPLICATION OF SEALANT AND COATING SYSTEM
 - 3.6.1 Preparation of Sealant and Coating Materials for Application
 - 3.6.1.1 Mixing Sealant, Primer and Intermediate Coat Materials
 - 3.6.1.2 Mixing Topcoat Material
 - 3.6.1.3 Pot Life
 - 3.6.1.4 Application Conditions and Recoat Windows
 - 3.6.2 Amine Blush Testing of Epoxy Coat Prior to Overcoating
 - 3.6.3 Application of Coating System and Joint Sealant
 - 3.6.3.1 Application of Primer
 - 3.6.3.2 Application of Stripe Coat
 - 3.6.3.3 Application of Intermediate Coat
 - 3.6.3.4 Non-skid for Stairs and Top
 - 3.6.3.5 Application of Topcoat
 - 3.6.3.6 Application of Joint Sealant
 - 3.6.3.7 Procedure for Holiday and Spot Repairs of Newly Applied Coating
 - 3.6.3.8 Structure Occupancy After Coating Application
- 3.7 PROJECT IDENTIFICATION
- 3.8 FIELD QUALITY CONTROL
 - 3.8.1 Coating Inspector
 - 3.8.2 Field Inspection

- 3.8.2.1 Inspection Requirements
- 3.8.2.2 Inspection Report Forms
- 3.8.2.3 Daily Inspection Reports
- 3.8.2.4 Inspection Logbook
- 3.8.2.5 Inspection Equipment
- 3.9 FINAL CLEANUP

-- End of Section Table of Contents --

SECTION 09 97 13.27

HIGH PERFORMANCE COATING FOR STEEL STRUCTURES

PART 1 GENERAL

1.1 REFERENCES

The publications listed below form a part of this specification to the extent referenced. The publications are referred to within the text by the basic designation only.

ASTM INTERNATIONAL (ASTM)

ASTM C920	(2018) Standard Specification for Elastomeric Joint Sealants
ASTM D1200	(2010; R 2014) Viscosity by Ford Viscosity Cup
ASTM D1640/D1640M	(2014) Standard Test Methods for Drying, Curing, or Film Formation of Organic Coatings
ASTM D3276	(2015; E 2016) Standard Guide for Painting Inspectors (Metal Substrates)
ASTM D3925	(2002; R 2015) Sampling Liquid Paints and Related Pigmented Coatings
ASTM D4285	(1983; R 2018) Indicating Oil or Water in Compressed Air
ASTM D7127	(2017) Standard Test Method for Measurement of Surface Roughness of Abrasive Blast Cleaned Metal Surfaces using a Portable Stylus Instrument
ASTM E11	(2024) Standard Specification for Woven Wire Test Sieve Cloth and Test Sieves

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO)

ISO 9001	(2015) Quality Management Systems- Requirements
----------	---

SOCIETY FOR PROTECTIVE COATINGS (SSPC)

SSPC 7/NACE No.4	(2007) Brush-Off Blast Cleaning
SSPC AB 2	(2015; E 2016) Cleanliness of Recycled Ferrous Metallic Abrasive
SSPC AB 3	(2023; R 2023) Ferrous Metallic Abrasive
SSPC Guide 6	(2021) Guide for Containing Surface Preparation Debris Generated During Paint Removal Operations
SSPC Guide 12	(2023) Guide for Illumination of Industrial Painting Projects
SSPC PA 1	(2024) Shop, Field, and Maintenance Coating of Metals

SSPC PA 2

(2015; E 2018) Procedure for Determining Conformance to Dry Coating Thickness Requirements

*AM0003

~~SSPC QP 4~~

~~(2019) Standard Procedure for Evaluating the Qualifications of Industrial/Marine Painting Contractors (Field Application to Complex Industrial Steel Structures and Other Metal Components)~~

AM0003*

SSPC QP 5

(2022) Standard Procedure for Evaluating the Qualifications of Coating and Lining Inspection Companies

SSPC QS 1

(2015) Standard Procedure for Evaluating a Contractor's Advanced Quality Management System

SSPC SP 1

(2015) Solvent Cleaning

SSPC SP 10/NACE No. 2

(2015) Near-White Blast Cleaning

SSPC SP COM

(2016; E 2017) Surface Preparation Commentary for Steel and Concrete Substrates

SSPC VIS 1

(2002; E 2004) Guide and Reference Photographs for Steel Surfaces Prepared by Dry Abrasive Blast Cleaning

SOCIETY OF AUTOMOTIVE ENGINEERS INTERNATIONAL (SAE)

SAE AMS-STD-595A

(2017) Colors used in Government Procurement

U.S. DEPARTMENT OF DEFENSE (DOD)

MIL-A-22262

(1993; Rev B; Am 1 1994; Am 2 1996; Notice 1 2021) Abrasive Blasting Media Ship Hull Blast Cleaning

MIL-DTL-24441

(2009; Rev D; Notice 1 2021) Paint, Epoxy-Polyamide, General Specification for

MIL-DTL-24441/19

(2009; Rev C; Notice 1 2023) Paint, Epoxy-Polyamide, Zinc Primer, Formula 159, Type III

MIL-DTL-24441/31

(2009; Rev B; Notice 1 2021) Paint, Epoxy-Polyamide, White, Formula 152, Type IV

MIL-PRF-85285

(2022; Rev F) Topcoat, Aircraft and Support Equipment

U.S. NATIONAL ARCHIVES AND RECORDS ADMINISTRATION (NARA)

29 CFR 1910.134

Respiratory Protection

29 CFR 1910.1000

Air Contaminants

29 CFR 1926.59

Hazard Communication

1.2 DEFINITIONS

Definitions are provided throughout this Section, generally in the paragraph where used, and denoted by capital letters.

1.3 SUBMITTALS

*AM0003 Government approval is required for submittals with a "G" or "S" classification. ~~Submittals not having a "G" or "S" classification are for Contractor Quality Control approval.~~ Submittals not having a "G" or "S" classification are for information only. When used, a code following the "G" classification identifies the office that will review the submittal for the Government. Submit the following in accordance with Section 01 33 00 SUBMITTAL PROCEDURES:

AM0003*

SD-05, Design Data

Containment System

SD-06 Test Reports

Joint Sealant Qualification Test Reports

Coatings Qualification Test Reports

Metallic Abrasive Qualification Test Reports

Coating Sample Test Reports

Abrasive Sample Test Reports

Inspection Report Forms

Daily Inspection Reports

Recycled Metallic Abrasive Field Test Reports (Daily and Weekly)

SD-07 Certificates

Contract Errors, Omissions, and Other Discrepancies

Corrective Action Procedures

Coating Work Plan

Qualifications of Certified Industrial Hygienist (CIH)

Qualifications Of Individuals Performing Abrasive Blasting

Qualifications of Certified Protective Coatings Specialist (PCS)

Qualifications of Coating Inspection Company

Qualifications of QC Specialist Coating Inspector

Qualifications of Testing Laboratory for Coatings

Qualifications of Testing Laboratory for Abrasive

Qualifications of Coating Contractors

Joint Sealant Materials

Coating Materials

Coating System Component Compatibility

Non-metallic Abrasive

Metallic Abrasive

SD-08 Manufacturer's Instructions

Joint Sealant Instructions

Coating System Instructions

SD-11 Closeout Submittals

Disposal of Used Abrasive

Inspection Logbook; G,

1.4 QUALITY ASSURANCE

1.4.1 Contract Errors, Omissions, and Other Discrepancies

Submit all errors, omissions, and other discrepancies in contract documents the Contracting Officer within 30 days of contract award for all work covered in this Section, other than the work that will not be uncovered until a later date. All such discrepancies shall be addressed and resolved, and the Coating Work Plan modified, prior to beginning the Initial and Follow-Up phases of work.

Discrepancies that become apparent only after work is uncovered shall be identified at the earliest discoverable time and submitted for resolution. Schedule time (Float) should be built into the project schedule at those points where old work is to be uncovered or where access is not available during the first 30 days after award, to allow for resolution of contract discrepancies.

1.4.2 Corrective Action (CA)

CA shall be included in the Quality Control Plan.

1.4.2.1 Corrective Action Procedures

Develop procedures for determining the root cause of each non-compliance, developing a plan to eliminate the root cause so that the non-compliance does not recur, and following up to ensure that the root cause was eliminated. Develop Corrective Action Request (CAR) forms for initiating CA, and for tracking and documenting each step.

1.4.2.2 Implement Corrective Action

The Contractor shall take action to identify and eliminate the root cause of each non-compliance so as to prevent recurrence. These procedures shall apply to non-compliance in the work, and to non-compliance in the QC System. Corrective actions shall be appropriate to the effects of the non-compliance encountered. Each CAR shall be serialized, tracked in a Log to completion and acceptance by the Contracting Officer, and retained in project records. The Corrective Action Log, showing status of each CAR, shall be submitted to the Contracting Officer monthly. A CAR may be initiated by either the Contractor or the Contracting Officer. The Contracting Officer must approve each CAR at the root cause identification stage, the plan for elimination stage, and the close out stage after verification that the root cause has been eliminated.

1.4.3 Coating Work Plan

This work plan shall be considered as part of the Quality Control Plan.

Provide procedures for reviewing contract documents immediately after award to identify errors, omissions, and discrepancies so that any such issues can be resolved prior to project planning and

development of detailed procedures.

Provide procedures for verification of key processes during Initial Phase to ensure that contract requirements can be met. Key processes shall include surface preparation, coating application and curing, inspection, and documentation, and any other process that might adversely impact orderly progression of work.

Provide procedures for all phases of coating operations, including planned work, rework, repair, inspection, and documentation. Address mobilization and setup, surface preparation, coating application, coating initial cure, tracking and correction of noncompliant work, and demobilization. Coordinate work processes with health and safety plans and confined space entry plans. For each process, provide procedures that include appropriate work instructions, material and equipment requirements, personnel qualifications, controls, and process verification procedures. Provide procedures for inspecting work to verify and document compliance with contract requirements, including inspection forms and checklists, and acceptance and rejection criteria.

Provide procedures for correcting noncompliant work. Detailed procedures are required in advance to avoid delays in meeting overcoat windows as well as to avoid delays in production. Provide procedures for repairing defects in the coating film, such as runs, drips, sags, holidays, overspray, as well as how to handle correct coating thickness noncompliance, any other areas of repair or rework that might be adversely affected by delays in preparing and approving new procedures.

If a procedure is based on a proposed or approved request for deviation, the deviation shall be referenced. Changes to procedures shall be noted by submittal number and date approved, clearly delineating old requirements and new requirements, so that the records provide a continuous log of requirements and procedures.

1.4.4 Design Data

1.4.4.1 Containment System

Submit complete design drawings and calculations for the scaffolding and containment system, including an analysis of the loads which will be added to the structure by the containment system and waste materials. A registered engineer shall approve calculations and scaffold system design.

1.4.5 Test Reports

1.4.5.1 Joint Sealant Qualification Test Reports

Submit test results from independent laboratory of representative samples of joint sealant material. Samples must have been tested within the last three years. Submit results as required in paragraph QUALITY ASSURANCE PROVISIONS of [ASTM C920](#). Note that testing in accordance with QUALITY ASSURANCE PROVISIONS is a pre-qualification requirement.

1.4.5.2 Coatings Qualification Test Reports

Submit test results from independent laboratory of representative samples of each coating material. U.S. Department of Defense laboratories are considered to be independent laboratories for purposes of compliance with "QUALIFICATION INSPECTION" requirements herein. Samples must have been tested within the last three years. Submit results for epoxy materials as required in paragraph QUALIFICATION INSPECTION of [MIL-DTL-24441](#), and as revised by paragraph COATING SYSTEM herein. Submit results for polyurethane materials as required in paragraph QUALIFICATION INSPECTION of [MIL-PRF-85285](#), and as revised by paragraph COATING SYSTEM herein. Note that requirement for QUALIFICATION INSPECTION is a pre-qualification requirement, and involves the same testing required for listing in the Qualified Products List of the respective material. See appropriate Military Specification for specific test requirements.

1.4.5.3 Metallic Abrasive Qualification Test Reports

Submit results for abrasive as required in paragraph 4 REQUIREMENTS of **SSPC AB 3**. Submit test results from independent laboratory of representative samples of each abrasive to be used on the jobsite. Samples must have been tested within the last three years. Note that this testing is for the purpose of prequalifying the abrasive.

1.4.5.4 Recycled Metallic Abrasive Field Test Reports (Daily and Weekly)

Submit test results from independent laboratory of daily and weekly Quality Control testing required by **SSPC AB 2**, as modified in paragraph ABRASIVE.

1.4.6 Qualifications

1.4.6.1 Qualifications of Certified Industrial Hygienist (CIH)

Submit name, address, telephone number, FAX number, and e-mail address of the independent third party CIH. Submit documentation that hygienist is certified by the American Board of Industrial Hygiene in comprehensive practice, including certification number and date of certification/recertification. Provide evidence of experience with hazards involved in industrial coating application work.

1.4.6.2 Qualifications of Certified Protective Coatings Specialist (PCS)

Submit name, address, telephone number, FAX number, and e-mail address of the independent third party PCS. Submit documentation that specialist is certified by SSPC: The Society for Protective Coatings (SSPC) as a PCS, including certification number and date of certification/recertification. If the PCS is employed by the same coating inspection company to which the coating inspector is employed, this does not violate the independent third-party requirements. The PCS shall remain certified during the entire project, and the Contracting Officer shall be notified of any change in certification status within 10 days of the change. The PCS shall not be the designated coating inspector.

1.4.6.3 Qualifications of Coating Inspection Company

Submit documentation that the coating inspection company that will be performing all coating inspection functions is certified by SSPC to the requirements of **SSPC QP 5** prior to contract award, and shall remain certified while accomplishing any coating inspection functions. The coating inspection company must remain so certified for the duration of the project. If a coating inspection company's certification expires, the firm will not be allowed to perform any inspection functions, and all surface preparation and coating application work must stop, until the certification is reissued. Requests for extension of time for any delay to the completion of the project due to an inactive certification will not be considered and liquidated damages will apply. Notify the Contracting Officer of any change in coating inspection company certification status.

1.4.6.4 Qualifications of QC Specialist Coating Inspector

Submit documentation that each coating inspector is employed, and qualified to **SSPC QP 5**, Level III, by the selected coating inspection company. Each inspector shall remain employed by the coating inspection company while performing any coating inspection functions.

1.4.6.5 Qualifications Of Individuals Performing Abrasive Blasting

Submit name, address, and telephone number of each person that will be performing abrasive blasting. Submit documentation that each blaster is qualified by SSPC to the SSPC C-7 Dry Abrasive Blaster Qualification Program. Each blaster shall remain qualified during the entire period of abrasive blasting, and the Contracting Officer shall be notified of any change in qualification status.

1.4.6.6 Qualifications of Testing Laboratory for Coatings

Submit name, address, telephone number, FAX number, and e-mail address of the independent third party laboratory selected to perform testing of coating samples for compliance with specification requirements. Submit documentation that laboratory is regularly engaged in testing of paint samples for conformance with specifications, and that persons performing analyses are qualified.

1.4.6.7 Qualifications of Testing Laboratory for Abrasive

Submit name, address, telephone number, FAX number, and e-mail address of the independent third party laboratory selected to perform testing of abrasive for compliance with specification requirements. Submit documentation that laboratory has experience in testing samples of abrasive for conformance with specifications, and that persons performing analyses are qualified.

1.4.6.8 Qualifications of Coating Contractors

AM0003** All Contractors and Subcontractors that perform surface preparation or coating application shall be certified to either **ISO 9001** ~~or SSPC QP 1~~ and **SSPC QS 1** prior to contract award, and shall remain certified while accomplishing any surface preparation or coating application. The painting Contractors and painting Subcontractors must remain so certified for the duration of the project. If a Contractor's or Subcontractor's certification expires, the firm will not be allowed to perform any work until the certification is reissued. Requests for extension of time for any delay to the completion of the project due to an inactive certification will not be considered and liquidated damages will apply. Notify the Contracting Officer of any change in Contractor certification status. **AM0003

1.4.6.9 Joint Sealant Materials

Provide manufacturer's certification of conformance to contract requirements.

1.4.6.10 Coating Materials

Provide manufacturer's certification of conformance to contract requirements.

1.4.6.11 Coating System Component Compatibility

Provide certification from each manufacturer of components of the coating system, epoxy primer, epoxy intermediate, and polyurethane topcoat, that the supplied coating material is suitable for use in the specified coating system. Each manufacturer shall identify the specific products, including manufacturer's name, which their product may be used with. The certification shall provide the name of the manufacturer that will provide technical support for the entire system. When all coating materials are manufactured by one manufacturer, this certification is not required.

1.4.6.12 Non-metallic Abrasive

Provide manufacturer's certification that the materials are currently approved by the Naval Sea Systems Command and listed on the Qualified Products Lists (QPL) for the specified materials.

1.4.6.13 Metallic Abrasive

Provide manufacturer's certification of conformance to contract requirements and provide copies of test results.

1.4.7 Protective Coating Specialist (PCS)

The PCS shall be considered a QC Specialist and shall report to the QC Manager, as specified in Section **01 45 00 QUALITY CONTROL**. The PCS shall approve all submittals prior to submission to the QC Manager for approval or submission to the government for approval.

1.4.8 Pre-Application Meeting

After approval of submittals but prior to the initiation of coating work, Contractor representatives, including at a minimum, project superintendent and QC manager, paint foreman, coating inspector, and PCS shall have a pre-application coating preparatory meeting. This meeting shall be in addition to the pre-construction conference. Specific items addressed shall include: corrective action requirements and procedures, coating work plan, safety plan, coordination with other Sections, inspection standards, inspection requirements and tools, test procedures, environmental control system, safety plan, and test logs. Notify Contracting Officer at least ten days prior to meeting.

1.5 PRODUCT DATA

1.5.1 Joint Sealant Instructions

Submit manufacturer's printed instructions including detailed application procedures, minimum and maximum application temperatures, and curing procedures. Include Safety Data Sheets (SDS) for materials to be used at the job site in accordance with [29 CFR 1926.59](#).

1.5.2 Coating System Instructions

Submit manufacturer's printed instructions including detailed mixing and application procedures, number and types of coats required, minimum and maximum application temperatures, and curing procedures. Include Safety Data Sheets (SDS) for materials to be used at the job site in accordance with [29 CFR 1926.59](#).

1.6 DELIVERY AND STORAGE

Ship, store, and handle materials in accordance with [SSPC PA 1](#), and as modified in this Section. Maintain temperature in storage spaces between [40 and 85 degrees F](#), and air temperature more than [5 degrees F](#) above the dew-point at all times. Inspect materials for damage prior to use and return non-compliant materials to manufacturer. Remove materials with expired shelf life from government property immediately and notify the Contracting Officer.

If materials are approaching shelf life expiration and an extension is desired, samples may be sent to the manufacturer, along with complete records of storage conditions, with a request for shelf life extension. If the manufacturer finds the samples and storage data suitable for shelf life extension, the manufacturer may issue an extension, referencing the product evaluation and the review of storage records. Products may not be extended longer than allowed in the product specification.

1.7 COATING HAZARDS

Ensure that employees are trained in all aspects of the safety plan. Specified coatings may have potential health hazards if ingested or improperly handled. The coating manufacturer's written safety precautions shall be followed throughout mixing, application, and curing of the coatings. During all cleaning, cleanup, surface preparation, and paint application phases, ensure that employees are protected from toxic and hazardous chemical agents which exceed concentrations in [29 CFR 1910.1000](#). Comply with respiratory protection requirements in [29 CFR 1910.134](#). The CIH shall approve work procedures and personal protective equipment.

1.8 JOB SITE REFERENCES

Make available to the Contracting Officer at least one copy each of [ASTM D3276](#), [ASTM D3925](#), [ASTM D4285](#), [ASTM D7127](#), [SSPC SP COM](#), [SSPC SP 1](#), [SSPC 7/NACE No.4](#), [SSPC SP 10/NACE No. 2](#), [SSPC PA 1](#), [SSPC PA 2](#), [SSPC Guide 6](#), [SSPC VIS 1](#), ~~[SSPC QP 1](#)~~, [SSPC QS 1](#), and an SSPC Certified Contractor Evaluation Form at the job site.

*AM0003

AM0003*

PART 2 PRODUCTS

2.1 JOINT SEALANT

TT-S-00230, Type II, Class B

2.2 COATING SYSTEM

Alternate systems or products will not be considered. Provide a complete system (primer, intermediate coat, top coat) material from one supplier.

Prepare surface and apply the complete coating system in the shop. Follow all temperature, humidity, and testing requirements listed herein.

The Military specification epoxy and polyurethane products specified in this Section do not require approval for listing on the QPL prior to contract award, as indicated in paragraph 3.2 of MIL-DTL-24441 and paragraph 3.1 of MIL-PRF-85285. Testing of products by an independent laboratory to the QUALIFICATION INSPECTION requirements of MIL-DTL-24441 and MIL-PRF-85285 prior to contract award is required. See specific submittal requirements in paragraph QUALITY ASSURANCE.

2.2.1 Zinc-Rich Epoxy Primer Coat

Epoxy polyamide, MIL-DTL-24441/19 (Formula 159, Type III).

2.2.2 Epoxy Intermediate Coat

Epoxy polyamide, MIL-DTL-24441/31 (Formula 152, Type IV, White (Tinted)). Tint to approximately SAE AMS-STD-595A color number 27778 parchment using pigment dispersions prepared for epoxy paint tinting. Manufacturer shall tint material and appropriately label. All other requirements of this Military Specification apply.

2.2.3 Polyurethane Topcoat

Polyurethane coating topcoat of MIL-PRF-85285, Type II, White SAE AMS-STD-595A color number 17925.

Modify paragraph 3.6.4 of MIL-PRF-85285, Viscosity and Pot Life, as follows:

The viscosity of the admixed coating, when tested in accordance with ASTM D1200 through a No. 4 Ford cup, shall be as follows:

Time from mix (minimum)	Maximum time through a No. 4 Ford cup
Initially	30 seconds
2 hours	60 seconds
4 hours	No gel

Modify paragraph 3.7.1 of MIL-PRF-85285, Drying Time, as follows:

When applied by spray techniques and when tested in accordance with ASTM D1640/D1640M, the coating shall be set-to-touch within four hours and dry-hard within eight hours (see 4.6 and table I).

2.3 COATING SAMPLE COLLECTION AND SHIPPING KIT

Provide a kit that contains one quart can for the base of each coating material, an appropriately sized

can for each activator, dipping cups for each component to be sampled, a shipping box sized for the samples to be shipped, and packing material. Mark cans for the appropriate component. Provide shipping documents, including either pre-paid shipping or a shipper number that can be used by the QC Manager to arrange pickup, addressed to the approved coating testing laboratory.

2.4 ABRASIVE SAMPLE COLLECTION AND SHIPPING KIT

Provide a kit that contains one suitable plastic bag or container for each sample to be collected. Mark containers for the appropriate component. Provide shipping documents, including either pre-paid shipping or a shipper number that can be used by the QC Manager to arrange pickup, addressed to the approved coating testing laboratory.

2.5 TEST KITS

2.5.1 Test Kit for Measuring Chloride, Sulfate and Nitrate Ions on Steel and Coated Surfaces

Provide test kits that meet all of the following requirements:

- a. Contains all materials, supplies, tools, and instructions for field testing and on-site quantitative evaluation of chloride, sulfate, and nitrate ions;
- b. Extract solution is acidic, factory pre-measured, pre-packaged, and of uniform concentration;
- c. Components and solutions are mercury free and environmentally friendly;
- d. Contains new materials and solutions for each test extraction;
- e. Contains an extraction test container (vessel, sleeve, cell) that creates a sealed, encapsulated environment during salt ion extraction;
- f. Contains a test extract container suitable for testing the following steel surfaces: horizontal (up/down configuration), vertical, flat, curved, smooth, pitted, and rough;
- g. All salt ion concentrations are directly measured in micrograms per square centimeter.

2.5.2 Test Kit for Identifying Amine Blush on Epoxy Surfaces

Provide test kits that meet all of the following requirements:

- a. Is a completely self-contained field test kit with all materials, supplies, tools, and instructions to perform tests and indicate the presence of unreacted amines;
- b. Uses an identifiable, consistent, uniform, pre-packaged, factory pre-measured indicating solution;
- c. Contains no mercury or lead and is environmentally friendly;
- d. Contains a solution of an unreacted amine for the purpose of "self checking" the indicator solution;

2.6 ABRASIVE

The referenced abrasive specifications have maximum limits for soluble salts contamination, however, this maximum level of contamination does not guarantee that contamination will not be transferred to the steel surface during abrasive blasting. Other factors such as on-site handling and recycling can allow contamination of abrasive. Contractors are cautioned to verify that the chosen abrasive, along with work and storage processes, allow the final surface cleanliness requirements to be achieved. Successful testing of chlorides in abrasive does not negate the final acceptance testing of steel surfaces.

2.6.1 Non-metallic Abrasive

Conform to [MIL-A-22262](#), Type I (Inorganic materials). Abrasive shall be approved by the Naval Sea Systems Command and listed on the appropriate Qualified Products List (QPL) for the specified materials. Use sampling procedures and testing frequencies as prescribed in [MIL-A-22262](#). Use abrasive that is specifically selected and graded to provide a sharp, angular profile to the specified depth. Do not use ungraded abrasive. Make adjustments to processes or abrasive gradation to achieve specified surface profile. Recycled non-metallic abrasive shall meet all requirements of the specification each time that it is placed in the blast pot.

2.6.2 Metallic Abrasive

2.6.2.1 New and Remanufactured Steel Grit

Conform to the chemical and physical properties of [SSPC AB 3](#) Class 1 (Steel) only. Class 2 (Iron) abrasive shall not be used.

To develop a suitable work mix from new steel abrasive, a minimum of 200 - 400 recycles is required, therefore, it is advantageous for a Contractor to use remanufactured steel grit or grit reclaimed from a previous project. Such grit shall be considered to conform if it can be traced to new grit conforming to [SSPC AB 3](#) Class 1 and it meets all cleanliness requirements of [SSPC AB 3](#) Class 1 when brought to the current jobsite. Submit one representative sample of this work mix to the laboratory for testing, along with samples of new material. Acceptance and use of this work mix shall not be used to justify any deviation from surface preparation requirements.

2.6.2.2 Recycled Steel Grit

Conform to the chemical and physical properties of [SSPC AB 2](#)

2.7 WHITE ALUMINUM OXIDE NON-SKID GRIT

Size #60, dust free (washed and dry), minimum 99 percent pure, having the following sieve analysis when tested in accordance with [ASTM E11](#) using a [2.2 pound](#) sample:

Sieve #	Percent Retained
40	0
50	15-40
60	60-85

PART 3 EXECUTION

Perform all work, rework, and repair in accordance with approved procedures in the Coating Work Plan.

3.1 COATING AND ABRASIVE SAMPLE COLLECTION AND TESTING

Sample and test materials delivered to the jobsite. Notify Contracting Officer three days in advance of sampling. The QC Manager and either the PCS or coating inspector shall witness all sampling.

3.1.1 Coating Sample Collection

Provide a sample collection kit as required in paragraph COATING SAMPLE COLLECTION AND SHIPPING KIT. From each lot, obtain a one [quart](#) sample of each base material, and proportional samples of each activator based on mix ratio, by random selection from sealed containers in accordance with [ASTM D3925](#). Prior to sampling, mix contents of each sealed container to ensure uniformity. As an alternative to collecting small samples from kits, entire kits may be randomly

selected and shipped to laboratory, observing all requirements for witnessing and traceability. For purposes of quality conformance inspection, a lot is defined as that quantity of materials from a single, uniform batch produced and offered for delivery at one time. A batch is defined as that quantity of material processed by the manufacturer at one time and identified by number on the label. Identify samples by designated name, specification number, batch number, project contract number, sample date, intended use, and quantity involved. The QC manager will take possession of the packaged samples, contact the shipping company to arrange for pickup, and relinquish the samples only to the shipping representative for shipment to the approved laboratory for testing as required by the paragraph COATING SAMPLE TEST REPORTS.

3.1.2 Abrasive Sample Collection

Provide a sample collection kit as required in paragraph ABRASIVE SAMPLE COLLECTION AND SHIPPING KIT. For purposes of quality conformance inspection, a lot shall consist of all abrasive materials of the same type from a single, uniform batch produced and offered for delivery at one time. Obtain samples of each abrasive lot using the sampling techniques and schedule of MIL-A-22262. The addition of any substance to a batch shall constitute a new lot. Identify samples by designated name, specification number, lot number, project contract number, sample date, intended use, and quantity involved. The QC manager will take possession of the packaged samples, contact the shipping company to arrange for pickup, and relinquish the samples only to the shipping representative for shipment to the approved laboratory for testing as required by the paragraph ABRASIVE SAMPLE TEST REPORTS.

3.1.3 Coating Sample Test Reports

Submit test results for each lot of coating material delivered to the jobsite. Test samples of primer, intermediate, and topcoat materials for compliance with requirements of Table I. Reject entire lot represented by samples that fail one or more tests, select new lots, and test samples.

3.1.4 Abrasive Sample Test Reports

Submit test results for each lot of abrasive delivered to the jobsite. Test samples of metallic abrasive to the requirements of paragraph REQUIREMENTS of SSPC AB 3, except paragraph 4.1.5 DURABILITY. Test samples of non-metallic abrasive as required in paragraph QUALITY CONFORMANCE INSPECTION of MIL-A-22262. Reject entire lot represented by samples that fail one or more tests, select new lots, and test samples.

3.2 SURFACES TO BE COATED

Shop coat exposed interior ferrous metal primary and secondary framing for Aircraft Maintenance Bays.

3.3 LIGHTING

Provide lighting for all work areas as prescribed in SSPC Guide 12.

3.4 ENVIRONMENTAL CONDITIONS

3.4.1 Containment

Design and provide a containment system for the capture, containment, collection, storage and disposal of the waste materials generated by the work under this Section, to meet the requirements of SSPC Guide 6, Class 1. Vapor concentrations shall be kept at or below 10 percent of Lower Explosive Limit (LEL) at all times. Containment may be designed as fixed containment for complete structure or portable containment for sections of structure, however, containment shall remain in any one place from beginning of abrasive blasting through initial cure of coating. Waste materials covered by this paragraph shall not include any material or residue from removal of coatings containing lead, chromium, cadmium, PCB, or any other hazardous material.

It is the Contractors responsibility to insure the feasibility and workability of the containment system.

The Contractor shall perform his operations and work schedule in a manner as to minimize leakage of the containment system. The containment system shall be properly maintained and shall not deviate from the approved drawings. If the containment system fails to function satisfactorily, the Contractor shall suspend all operations, except those required to minimize adverse impact on the environment or government property. Operations shall not resume until modifications have been made to correct the cause of the failure.

3.4.2 Automated Monitoring Requirements

Provide continuous monitoring of temperature, relative humidity, and dew point data at pertinent points on the structure, during surface preparation, coating application, and initial cure. Locate sensors to provide pertinent data for the surface preparation and coat application being performed. Monitor any heating, cooling, or dehumidification equipment used. Make data available to the Contracting Officer through Internet access. Provide monitoring equipment to perform as follows:

- a. Data is collected in the field unit in one minute increments, and available for download (on-site) in a standard format. Contractor shall collect this data and make available to the Contracting Officer;
- b. Monitoring equipment shall have backup power such that data collection and transmission to web server will be uninterrupted during the entire period of the dehumidification requirement;
- c. Monitoring equipment shall have capability to measure surface temperatures at a minimum of four locations anywhere on a 150 foot diameter by 50 foot high tank;
- d. Monitoring equipment shall have capability to measure interior and exterior dry bulb temperature (DB), relative humidity (RH), and dewpoint temperature (DP);
- e. Data shall be available continuously through secure Internet connection, using widely available web browsers;
- f. Internet accessible data shall be collected and stored in maximum 15 minute increments, and lag time between data collection and online availability shall be no greater than 70 minutes;
- g. Internet accessible data shall be available for viewing online in tabular format, and graphical format using selected data;
- h. Internet accessible data shall be available for download in user-defined segments, or entire project to date, in a standard format usable by Microsoft Excel and other spreadsheet programs.
- i. Internet-based controls shall provide alerts to pre-designated parties through email messaging;
- j. Internet-based controls shall monitor data uploads from field unit and issue alert if data not initiated within 60 minutes of last upload;
- k. Internet-based controls shall monitor operation of DH equipment and issues alert when power remains off for more than 15 seconds, or if pre-determined temperature, RH, or DP conditions are exceeded;

The requirements listed here were developed around the Munters Exactaire Monitoring System, as this was the only monitoring system having Internet connectivity known to be commercially available. There is no requirement for connectivity of the monitoring system to control the DH equipment, therefore, any combination of equipment having the required functionality will be accepted.

3.5 SURFACE PREPARATION

3.5.1 Abrasive Blasting Equipment

Use abrasive blasting equipment of conventional air, force-feed, or pressure type. Maintain a minimum pressure of 95 psig at nozzle. Confirm that air supply for abrasive blasting is free of oil and

moisture when tested in accordance with [ASTM D4285](#). Test air quality at each startup, but in no case less often than every five operating hours.

3.5.2 Operational Evaluation of Abrasive

Test abrasive for salt contamination and oil contamination as required by the appropriate abrasive specification daily at startup and every five operating hours thereafter.

3.5.3 Surface Standard

Inspect surfaces to be coated, and select plate with similar properties and surface characteristics for use as a surface standard. Blast clean one or more [one foot](#) square steel panels as specified in paragraph SURFACE PREPARATION. Record blast nozzle type and size, air pressure at nozzle and compressor, distance of nozzle from panel, and angle of blast to establish procedures for blast cleaning. Measure surface profile in accordance with [ASTM D7127](#). When the surface standard complies with all specified requirements, seal with a clearcoat protectant. Use the surface standard for comparison to abrasive blasted surfaces throughout the course of work.

3.5.4 Pre-Preparation Testing for Surface Contamination

Perform testing, abrasive blasting, and testing in the prescribed order.

3.5.4.1 Pre-Preparation Testing for Oil and Grease Contamination

Inspect all surfaces for oil and/or grease contamination using two or more of the following inspection techniques: 1) Visual inspection, 2) WATER BREAK TEST, 3) CLOTH RUB TEST. Reject oil and/or grease contaminated surfaces, clean in accordance with [SSPC SP 1](#), and recheck for contamination until surfaces are free of oil and grease.

WATER BREAK TEST - Spray atomized mist of distilled water onto surface, and observe for water beading. If water "wets" surface rather than beading up, surface can be considered free of oil or grease contamination. Beading of water (water forms droplets) is evidence of oil or grease contamination.

CLOTH RUB TEST - Rub a clean, white, lint free, cotton cloth onto surface and observe for discoloration. To confirm oil or grease contamination in lightly stained areas, a non-staining solvent may be used to aid in oil or grease extraction. Any visible discoloration is evidence of oil or grease contamination.

3.5.4.2 Pre-Preparation Testing for Soluble Salts Contamination

Test surfaces for soluble salts, and wash as required, prior to abrasive blasting. Soluble salt testing is also required in paragraph PRE-APPLICATION TESTING FOR SOLUBLE SALTS CONTAMINATION as a final acceptance test of prepared surfaces after abrasive blasting, and successful completion of this phase does not negate that requirement. This phase is recommended since pre-preparation testing and washing are generally more advantageous than attempting to remove soluble salt contamination after abrasive blasting. Effective removal of soluble salts will require removal of any barrier to the steel surface, including rust. This procedure may necessitate combinations of wet abrasive blasting, high pressure water rinsing, and cleaning using a solution of water washing and soluble salts remover. The soluble salts remover shall be acidic, biodegradable, nontoxic, noncorrosive, and after application, will not interfere with primer adhesion. Delays between testing and preparation, or testing and coating application, may allow for the formation of new contamination. Use potable water, or potable water modified with soluble salt remover, for all washing or wet abrasive blasting. Test methods and equipment used in this phase are selected at the Contractor's discretion.

3.5.5 Abrasive Blasting

Abrasive blast steel surfaces to near-white metal in accordance with [SSPC SP 10/NACE No. 2](#). Prepared surfaces shall conform to [SSPC VIS 1](#) and shall match the prepared test-panels. Provide a

2 to 3 mil surface profile. Reject profile greater than 3 mils, discontinue abrasive blasting, and modify processes and materials to provide the specified profile. Measure surface profile in accordance with ASTM D7127, using Rmax as the measure of profile height. Record all measurements required in this standard. Measure profile at rate of three test areas for the first 1000 square feet plus one test area for each additional 1000 square feet or part thereof. When surfaces are reblasted for any reason, retest profile as specified. Following abrasive blasting, remove dust and debris by vacuum cleaning. Do not attempt to wipe surface clean.

3.5.6 Disposal of Used Abrasive

Dispose of used abrasive off Government property in accordance with Federal, State, and Local mandated regulations.

3.5.7 Pre-Application Testing For Surface Contamination

3.5.7.1 Pre-Application Testing for Oil and Grease Contamination

Ensure surfaces are free of contamination as described in paragraph PRE-PREPARATION TESTING FOR OIL AND GREASE CONTAMINATION, except that only questionable areas need be checked for beading of water misted onto surface.

3.5.7.2 Pre-Application Testing for Soluble Salts Contamination

Test surfaces for chloride contamination using the Test Kit described in TEST KIT FOR MEASURING CHLORIDE, SULFATE AND NITRATE IONS ON STEEL AND COATED SURFACES. Test all surfaces at rate of three tests for the first 1000 square feet plus one test for each additional 2000 square feet or part thereof. Perform 30 percent of tests on bare steel at welds, divided equally between horizontal and vertical welds. One or more readings greater than 3 micrograms per square centimeter of chlorides or 10 micrograms per square centimeter of sulfates or 5 micrograms per square centimeter of nitrates is evidence of soluble salt contamination. Reject contaminated surfaces, wash as discussed in paragraph PRE-PREPARATION TESTING FOR SOLUBLE SALTS CONTAMINATION, allow to dry, and re-test until all required tests show allowable results. Reblast tested and cleaned areas as required. Label all test tubes and retain for test verification.

3.5.7.3 Pre-Application Testing for Surface Cleanliness

Apply coatings to dust free surfaces. To test surfaces, apply strip of clear adhesive tape to surface and rub onto surface with finger. When removed, the tape should show little or no dust, blast abrasive, or other contaminant. Reject contaminated surfaces and retest. Test surfaces at rate of three tests for the first 1000 square feet plus one test for each additional 1000 square feet or part thereof. Provide two additional tests for each failed test or questionable test. Attach test tapes to Daily Inspection Reports.

3.6 MIXING AND APPLICATION OF SEALANT AND COATING SYSTEM

3.6.1 Preparation of Sealant and Coating Materials for Application

Each of the sealant, primer, intermediate, and topcoat materials is a two-component material supplied in separate containers.

3.6.1.1 Mixing Sealant, Primer and Intermediate Coat Materials

Mix in accordance with manufacturer's instructions, which may differ for each product. Do not mix partial kits, or alter mix ratios. Mix materials in same temperature and humidity conditions specified in paragraph DELIVERY AND STORAGE. Allow mixed material to stand for the required induction time based on its temperature.

3.6.1.2 Mixing Topcoat Material

Do not mix partial kits, or alter mix ratios. Mix polyurethane coating materials in same temperature conditions specified in paragraph DELIVERY AND STORAGE. The polyurethane coating material is moisture sensitive and any introduction of moisture or water into the material during mixing or application will shorten usable pot life. Use a mixer that does not create a vortex. Do not add solvent without specific written recommendation from the manufacturer. No induction time is required, only thorough agitation of the mixed material.

3.6.1.3 Pot Life

Apply mixed products within stated pot life for each product. Stop applying when material becomes difficult to apply in a smooth, uniform wet film. Add all required solvent at time of mixing. Do not add solvent to extend pot life. Pot life is based on standard conditions at 70 degrees F and 50 percent relative humidity. For every 18 degrees F rise in temperature, pot life is reduced by approximately half, and for every 18 degrees F drop it is approximately doubled. Usable pot life depends on the temperature of the material at the time of mixing and the sustained temperature at the time of application. Other factors such as the shape of the container and volume of mixed material may also affect pot life. Precooling or exterior icing of components for at least 24 hours to a minimum of 50 degrees F in hot climates will extend pot life. High humidity at time of mixing and application shortens pot life of the Polyurethane topcoat material. Following are approximate pot life times:

Sealant	As specified by manufacturer
Epoxy primer and intermediate materials	4 hours
Polyurethane topcoat materials	2 hours.

3.6.1.4 Application Conditions and Recoat Windows

The application condition requirements for the coating system are very time and temperature sensitive, and are intended to avoid the delamination problems frequently found on industrial structures. Plan coating application to ensure that specified temperature, humidity, and condensation conditions are met. If conditions do not allow for orderly application of sealant, primer, stripe coat, intermediate coat and topcoat, use appropriate means of controlling air and surface temperatures, as required. Partial or total enclosures, insulation, heating or cooling, or other appropriate measures may be required to control conditions to allow for orderly application of all required coats.

Maintain air and steel surface temperature between 60 and 100 degrees F during application and the first four hours of cure for epoxy coats and the first eight hours of cure for polyurethane coats. Maintain steel surface temperature more than 5 degrees F above the dew-point of the ambient air for the same period.

Use Table entitled "RECOAT WINDOWS" to determine appropriate recoat windows for each coat after the initial coat. Apply each coat during appropriate RECOAT WINDOW of preceding coat. If a RECOAT WINDOW is missed, the minimum and maximum primer and intermediate coat thickness may be adjusted to accommodate a FILL COAT, however, requirements for total epoxy coating thickness and total coating thickness will not be modified. Missing more than one RECOAT WINDOW may require complete removal of coating if maximum total coating thickness requirements cannot be achieved.

If coating is not applied during RECOAT WINDOW, or if surface temperature exceeds 120 degrees F between applications, provide GLOSS REMOVAL, apply next coat within 24 hours. If next planned coat is topcoat, apply FILL COAT if required to fill sanding marks. Sanding marks from GLOSS REMOVAL of intermediate coat reflecting through topcoat will be considered as noncompliant. Apply FILL COAT within 24 hours of GLOSS REMOVAL, then apply topcoat within RECOAT WINDOW of FILL COAT.

RECOAT WINDOWS						
<u>EPOXY OVER EPOXY</u>						
Temperature degrees F	60-70	71-80	12-36	91-100	101-110	111-120
RECOAT WINDOW (Hrs.)	24-72	18-60	16-48	12-36	8-18	4-6
<u>POLYURETHANE OVER EPOXY</u>						
Temperature degrees F	60-70	71-80	12-36	91-100	101-110	111-120
RECOAT WINDOW (Hrs.)	24-96	24-72	16-48	12-36	10-24	8-16
<u>POLYURETHANE OVER POLYURETHANE</u>						
Temperature degrees F	60-70	71-80	12-36	91-100	101-110	111-120
RECOAT WINDOW (Hrs.)	8-48	6-48	4-36	3-24	2-12	1-2

The temperature ranges shown in the table above are for determining recoat windows. Choose recoat window based on the highest surface temperature that was sustained for one or more hours between coats. This applies to the entire time between coats. Measure and record air and surface temperatures on hourly basis to determine appropriate recoat windows. If surface temperature goes above **100 degrees F**, measure and record temperatures every half hour.

FILL COAT - Where indicated, apply coat of intermediate coat epoxy, at **2 to 3 mils** DFT, then apply next specified full coat within recoat window of **FILL COAT**. A **FILL COAT** may be used to adjust coating thickness to comply with requirements or to fill sanding marks in intermediate coat.

GLOSS REMOVAL - Where required, hand sand in a linear fashion to remove gloss using 120-200 grit wet/dry sandpaper, followed by solvent wiping with a clean rag soaked with denatured alcohol to

remove all dust. GLOSS REMOVAL of primer coat is to scarify surface and shall consist of removal of approximately 1 mil of coating. If steel is exposed during GLOSS REMOVAL, repair in accordance with paragraph PROCEDURE FOR HOLIDAY AND SPOT REPAIRS OF NEWLY APPLIED COATING. GLOSS REMOVAL of intermediate coat may include removal of up to 3 mils of coating to avoid excess thickness, prior to application of FILL COAT.

3.6.2 Amine Blush Testing of Epoxy Coat Prior to Overcoating

Test epoxy surfaces prior to application of roof joint sealant, epoxy coat, or polyurethane topcoat for amine blush contamination using the Test Kit described in paragraph TEST KIT FOR IDENTIFYING AMINE BLUSH ON EPOXY SURFACES. Test all surfaces at rate of three tests for the first 1000 square feet plus one test for each additional 2000 square feet or part thereof. Remove any identified contamination using an approved procedure.

3.6.3 Application of Coating System and Joint Sealant

Apply coatings in accordance with SSPC PA 1 and as specified herein. Apply coatings to surfaces that meet all stated surface preparation requirements.

After application of primer coat and prior to application of each subsequent coat, perform testing prescribed in paragraph PRE-APPLICATION TESTING FOR SURFACE CONTAMINATION, as necessary, to ensure minimal intercoat contamination. This testing may be reduced to one half of the prescribed rate for bare steel if the testing indicates no contamination when sampling is evenly distributed over surfaces being tested. If contamination is found between coats, revert to the specified testing rate. Generally, oil and grease contamination and soluble salts contamination are not encountered if subsequent coats are applied within specified recoat windows and unusual atmospheric events do not occur. Such atmospheric events as a coastal storm blowing onshore can bring unusual chloride contamination. Concern for intercoat contamination should be continually prevalent, and spot testing should be accomplished to verify satisfactory conditions. Where visual examination or spot testing indicates contamination, perform sufficient testing to verify non-contamination, or to define extent of contamination for appropriate treatment.

Apply each coat in a consistent wet film, at 90 degrees to previous coat. Ensure that primer and intermediate coat "cold joints" are no less than six inches from welds. Apply stripe coat by brush. For convenience, stripe coat material may be delivered by spray if followed immediately with brush-out and approved procedures include appropriate controls on thickness. Apply all other coats by spray application. Use appropriate controls to prevent airborne coating fog from drifting beyond 15 feet from the structure perimeter. Cover or protect all surfaces that will not be coated. The cleanliness, temperature, recoat windows, and airborne paint containment requirements may necessitate the use of enclosures, portable shelters, or other appropriate controls.

Apply coatings at the following specified thickness:

Coat	Minimum DFT (Mils)	Maximum DFT (Mils)
Primer	3	5
Intermediate	3	5
Top	2	3
Total system	8	13

3.6.3.1 Application of Primer

Apply primer coat, maintaining paint supply container height within 3 feet of the paint nozzle for applying zinc primer. Maintain constant agitation of paint pot to ensure that zinc does not settle in container.

3.6.3.2 Application of Stripe Coat

Apply a stripe coat of intermediate coat epoxy material within RECOAT WINDOW of primer, allowing sufficient dry time to allow application of intermediate coat within RECOAT WINDOW of primer. Apply by brush, working material into corners, crevices, angles, and welds, and onto outside corners and angles.

3.6.3.3 Application of Intermediate Coat

Apply intermediate coat within RECOAT WINDOW of primer coat.

3.6.3.4 Non-skid for Stairs and Top

Where non-skid is required, apply a second intermediate coat, and immediately follow with application of non-skid grit, broadcast at the rate of 2 pounds per 100 square feet, and backroll. Apply topcoat as specified.

3.6.3.5 Application of Topcoat

Make all required repairs to primer and intermediate coats as specified in paragraph entitled "Procedure for Holiday and Spot Repairs of Newly Applied Coating" prior to applying topcoat. Apply topcoat within RECOAT WINDOW of intermediate coat. The polyurethane topcoat may require multiple passes to achieve desired aesthetics and required thickness. Consult manufacturer for thinning and application procedures for anticipated temperature, humidity, and wind conditions. Touch-up blemishes and defects within recoat window of polyurethane topcoat. Retain sample of polyurethane topcoat, from the same batch used to coat structure, to make touch-ups that might be required later.

3.6.3.6 Application of Joint Sealant

Apply joint sealant to back-to-back steel joints that are less than 3/8 inches wide and are not seal welded. Apply sealant to top and bottom, or each side, of narrow joints. Apply sealant within 48 hours of application of the topcoat, and touch-up with topcoat after appropriate cure of the sealant.

3.6.3.7 Procedure for Holiday and Spot Repairs of Newly Applied Coating

Repair coating film defects at the earliest practicable time, preferably before application of the succeeding coat. Observe all requirements for soluble salts contamination, cleanliness between coats, and application conditions. Prepare defective area in accordance with [SSPC SP 10/NACE No. 2](#), and feather coating as required to leave [4 inches](#) of each succeeding coat feathered and abraded. Protect adjacent areas from damage and overspray. Remove dust and solvent wipe the prepared area plus an additional [4 inches](#) beyond the prepared area with clean denatured alcohol. Apply each coat within RECOAT WINDOW of preceding coat. Within four hours of preparation, apply zinc-rich primer to prepared steel and feather onto prepared primer. Apply intermediate coat to primed area and feather to prepared intermediate area. Apply topcoat to intermediate coat and feather to prepared topcoat. Apply each repair coat to approximate thickness of surrounding coating system.

3.6.3.8 Structure Occupancy After Coating Application

Use clean canvas or other approved shoe covers when walking on coated surfaces, regardless of curing time allowed. For heavily trafficked areas, provide cushioned mats for additional protection.

3.7 PROJECT IDENTIFICATION

At the completion of the work, stencil the following information on the structure in 3/4 to one inch Helvetica style letters of contrasting color using acrylic stencil paint:

Date exterior coated:

Project Number:
Contractor:
Address:
Coating System
Surface Prep: SSPC SP _____ Profile: _____
Primer: _____ Thickness: _____
Intermediate: _____ Thickness: _____
Topcoat: _____ Thickness: _____
Total Thickness: _____

3.8 FIELD QUALITY CONTROL

For marking of tank surfaces, use chalk for marking bare steel, and water based markers for marking coated surfaces, and remove marks prior to coating. Do not use any wax or grease based markers, or any other markers that leave a residue or stain.

3.8.1 Coating Inspector

The coating inspector shall be considered a QC Specialist and shall report to the QC Manager, as specified in Section 01 45 00 QUALITY CONTROL. The Coating Inspector shall be present during all pre-preparation testing, surface preparation, coating application, initial cure of the coating system, during all coating repair work, and during completion activities as specified in Section 01 45 00 QUALITY CONTROL. The Coating Inspector shall provide complete documentation of conditions and occurrences on the job site, and be aware of conditions and occurrences that are potentially detrimental to the coating system. The requirements for inspection listed in this Section are in addition to the QC inspection and reporting requirements specified in Section 01 45 00 QUALITY CONTROL.

3.8.2 Field Inspection

3.8.2.1 Inspection Requirements

Perform field inspection in accordance with ASTM D3276 and the approved Coating Work Plan. Document Contractor's compliance with the approved Coating Work Plan.

Provide all tools and instruments required to perform the required testing, as well as any tools or instruments that the inspector considers necessary to perform the required inspections and tests. Document each inspection and test, including required hold points and other required inspections and tests, as well as those inspections and tests deemed prudent from on-site evaluation to document a particular process or condition, as follows:

- a. Location or area;
- b. Purpose (required or special);
- c. Method;
- d. Criteria for evaluation;
- e. Results;
- f. Determination of compliance;
- g. List of required rework;
- h. Observations.

Collect and record Environmental Conditions as described in ASTM D3276 on a 24 hour basis, as follows:

- a. During surface preparation, every two hours or when changes occur;
- b. During coating application and the first four days of initial cure, every hour, or when changes occur;
- c. Note location, time, and temperature of the highest and lowest surface temperatures each day;
- d. Use a non-contact thermometer to locate temperature extremes, then verify with contact

thermometers.

Document all equipment used in inspections and testing, including manufacturer, model number, serial number, last calibration date and future calibration date, and results of on-site calibration performed.

Document Contractors compliance with the approved Coating Work Plan.

3.8.2.2 Inspection Report Forms

Develop project-specific report forms as required to report measurements, test results, and observations being complete and conforming to contract requirements. This includes all direct requirements of the contract documents and indirect requirements of referenced documents. Show acceptance criteria with each requirement and indication of conformity of each inspected item. The data may be in any format, but must be legible and presented so that entered data can be quickly compared to the appropriate requirement.

3.8.2.3 Daily Inspection Reports

Submit one copy of daily inspection report completed each day when performing work under this Section, to the Contracting Officer. Note all non-compliance issues, and all issues that were reported for rework in accordance with QC procedures of Section 01 45 00 QUALITY CONTROL. Each report shall be signed by the coating inspector and the QC Manager. Submit report within 24 hours of date recorded on the report.

3.8.2.4 Inspection Logbook

A continuous record of all activity related to this Section shall be maintained in an Inspection Logbook on a daily basis. The logbook shall be hard or spiral bound with consecutively numbered pages, and shall be used to record all information provided in the Daily Inspection Reports, as well as other pertinent observations and information. The Coating Inspector's Logbook that is sold by NACE is satisfactory. Submit the original Inspection Logbook to the Contracting Officer upon completion of the project and prior to final payment.

3.8.2.5 Inspection Equipment

All equipment shall be in good condition, operational within its design range, and calibrated as required by the specified standard for use of each device.

3.9 FINAL CLEANUP

Following completion of the work, remove debris, equipment, and materials from the site. Remove temporary connections to Government or Contractor furnished water and electrical services. Restore existing facilities in and around the work areas to their original condition.

TABLE 1						
COATING QUALITY CONFORMANCE INSPECTION REQUIREMENTS						
Table 1a - Zinc-rich Epoxy Primer Coat MIL-DTL-24441/19 Formula 159						
<u>Test</u>	<u>Component A</u>		<u>Component B</u>		<u>Mixed</u>	
	<u>Min.</u>	<u>Max.</u>	<u>Min.</u>	<u>Max.</u>	<u>Min.</u>	<u>Max.</u>
Pigment content, percent (zinc dust)	---	---	81.5	85.5	---	---
Volatiles, percent	42.8	44.3	8.0	8.4	---	---
Non-volatile vehicle percent	53.7	57.7	8.3	8.7	---	---
Weight, Kilograms/liter	0.87	1.01	3.30	3.40	2.80	2.91
Weight, Pounds/gallon	7.3	8.4	27.5	28.4	23.4	24.4
Flashpoint, Degrees C	35.6	---	37.8	---	---	---
Flashpoint, Degrees F	96	---	100	---	---	---
Consistency, grams	---	---	250	500	150	300
Set to touch time, hours at 23 degrees C, 73 degrees F	---	---	---	---	---	2
Dry hard time, hours at 23 degrees C, 73 degrees F	---	---	---	---	---	8
Pot life, hours at 23 degrees C, 73 degrees F	---	---	---	---	4	---
Sag resistance, Micrometers	---	---	---	---	300	---
Sag resistance, Mils	---	---	---	---	12	---
VOC, Grams/liter	---	---	---	---	---	304
VOC, Pounds/gallon	---	---	---	---	---	2.5

TABLE 1						
COATING QUALITY CONFORMANCE INSPECTION REQUIREMENTS						
Table 1a - Zinc-rich Epoxy Primer Coat MIL-DTL-24441/19 Formula 159						
<u>Test</u>	<u>Component A</u>		<u>Component B</u>		<u>Mixed</u>	
	<u>Min.</u>	<u>Max.</u>	<u>Min.</u>	<u>Max.</u>	<u>Min.</u>	<u>Max.</u>
NOTES: Test methods as specified in MIL-DTL-24441 .						

TABLE 1						
COATING QUALITY CONFORMANCE INSPECTION REQUIREMENTS						
Table 1b - Epoxy Intermediate Coat <u>MIL-DTL-24441/31</u> Formula 152 Type IV (White (Tinted))						
<u>Test</u>	<u>Component A</u>		<u>Component B</u>		<u>Mixed</u>	
	<u>Min.</u>	<u>Max.</u>	<u>Min.</u>	<u>Max.</u>	<u>Min.</u>	<u>Max.</u>
Pigment content, percent	44.0	49.0	33.0	38.0	---	---
Volatiles, percent	29.0	35.0	16.0	21.0	---	---
Non-volatile vehicle percent	17.5	23.5	44.0	49.0	---	---
Coarse particles, percent	---	0.3	---	0.3	---	---
Consistency, grams	180	320	300	470	180	245
Weight, Kilograms/liter	1.39	1.45	1.29	1.35	1.34	1.4
Weight, Pounds/gallon	11.6	12.1	10.8	11.3	11.2	11.7
Set to touch time, hours at 23 degrees C, 73 degrees F	---	---	---	---	---	3
Dry hard time, hours at 23 degrees C, 73 degrees F	---	---	---	---	---	8
Fineness of grind, Hegman	4	---	4	---	---	---
Flashpoint, Degrees C	35.5	---	37.8	---	---	---
Flashpoint, Degrees F	96	---	100	---	---	---
Titanium dioxide, percent of pigment	91	---	---	---	---	---
Pot life, hours at 23 degrees C, 73 degrees F	---	---	---	---	4	---
Sag resistance, Micrometers	---	---	---	---	300	---
Sag resistance, Mils	---	---	---	---	12	---

TABLE 1						
COATING QUALITY CONFORMANCE INSPECTION REQUIREMENTS						
Table 1b - Epoxy Intermediate Coat MIL-DTL-24441/31 Formula 152 Type IV (White (Tinted))						
Test	Component A		Component B		Mixed	
	Min.	Max.	Min.	Max.	Min.	Max.
Color of dry film to approximate color of SAE AMS-STD-595A color 27778	---	---	---	---	---	Conform
Contrast ratio, at 75 micrometers, 3 mils DFT	---	---	---	---	.098	---
Gloss, 60 degree specular	---	---	---	---	35	---
VOC, Grams/liter	---	---	---	---	---	340
VOC, Pounds/gallon	---	---	---	---	---	2.8
GENERAL NOTES: Test methods as specified in MIL-DTL-24441. Where "Conform" is indicated, refer to specific requirements of MIL-DTL-24441/31.						

TABLE I						
COATING QUALITY CONFORMANCE INSPECTION REQUIREMENTS						
Table Ic - Polyurethane TopcoatMIL-PRF-85285 Type II (White and Colors)						
Test	Component A		Component B		Mixed	
	Min.	Max.	Min.	Max.	Min.	Max.
Moisture content, percent	---	2	---	---	---	---
Course particles, percent	---	---	---	---	---	.5
Viscosity	---	---	---	---	---	See Note 1
Fineness of grind, Hegman	---	---	---	---	7	---
Drying to touch (See Note 2)	---	---	---	---	---	4
Dry-hard (See Note 2)	---	---	---	---	---	8
VOC, grams per liter	---	---	---	---	---	340
Color	---	---	---	---	delta E+/-1.0	
Gloss 60 degree specular gloss						
Gloss	---	---	---	---	---	90
Semi-gloss	---	---	---	---	15	45
Opacity	---	---	---	---	0.95	---
Flexibility	---	---	---	---	---	Conform
Fluid resistance	---	---	---	---	---	Conform
Heat resistance (cure)	---	---	---	---	---	Conform
Solvent resistance (cure)	---	---	---	---	---	Conform
Condition in container	---	---	---	---	---	Conform
Odor	---	---	---	---	---	Conform
Lead percent	---	---	---	---	---	0.06
Cadmium percent	---	---	---	---	---	0.06

TABLE I						
COATING QUALITY CONFORMANCE INSPECTION REQUIREMENTS						
Table Ic - Polyurethane TopcoatMIL-PRF-85285 Type II (White and Colors)						
Test	Component A		Component B		Mixed	
	Min.	Max.	Min.	Max.	Min.	Max.
Chromium percent	---	---	---	---	---	0.00
NOTES: (1) Modify paragraph 3.6.4 Viscosity and Pot Life, of MIL-PRF-85285 as follows: The viscosity of the admixed coating, when tested in accordance with ASTM D1200 through a No. 4 Ford cup, shall be as follows:						
Time from mix (minimum)			Maximum time through a No. 4 Ford Cup			
Initially			30 seconds			
2 hours			60 seconds			
4 hours			No gel			
(2) Modify paragraph 3.7.1 Drying Time, of MIL-PRF-85285. When applied by spray techniques and when tested in accordance with ASTM D1640/D1640M, the coating shall be set-to-touch within four hours and dry-hard within eight hours (see 4.6 and table I).						
GENERAL NOTES: Test methods as specified in MIL-PRF-85285, except those marked with "***". Where "Conform" is indicated, refer to specific requirements of MIL-PRF-85285.						

-- End of Section --

SECTION TABLE OF CONTENTS

DIVISION 25 - INTEGRATED AUTOMATION

SECTION 25 05 11.01

CYBERSECURITY FOR FACILITY-RELATED CONTROL SYSTEMS: HVAC

PART 1 GENERAL

- 1.1 CONTROL SYSTEM APPLICABILITY
- 1.2 RELATED REQUIREMENTS
- 1.3 REFERENCES
- 1.4 DEFINITIONS
 - 1.4.1 Administrator Account
 - 1.4.2 Computer
 - 1.4.3 Controller
 - 1.4.4 Mission Space
 - 1.4.5 Network
 - 1.4.6 Network Connected
 - 1.4.6.1 Wireless Network Connected
 - 1.4.7 Network Media
 - 1.4.8 User Account Support Levels
 - 1.4.8.1 FULLY Supported
 - 1.4.8.2 MINIMALLY Supported
 - 1.4.8.3 NOT Supported
 - 1.4.9 Manual Local Input
 - 1.4.10 Card Reader
 - 1.4.11 User Interface
 - 1.4.11.1 Local User Interface
 - 1.4.11.2 Remote User Interface
 - 1.4.11.3 Types of User Interface (by capability)
 - 1.4.11.3.1 Read-Only User Interface
 - 1.4.11.3.2 Limited User Interface
 - 1.4.11.3.3 Full User Interface
 - 1.4.11.3.4 View-Only User Interface
 - 1.4.11.4 Other User Interface Terminology
 - 1.4.11.4.1 Writable User Interface
 - 1.4.11.4.2 Privileged User Interface
 - 1.4.12 Wireless Network
 - 1.4.13 Wired Broadcast Network
- 1.5 ADMINISTRATIVE REQUIREMENTS
 - 1.5.1 Points of Contact
 - 1.5.2 Coordination
- 1.6 SUBMITTALS
- 1.7 CYBERSECURITY DOCUMENTATION
 - 1.7.1 Proposed STIG and SRG Applicability Report
 - 1.7.2 Cybersecurity Interconnection Schedule
 - 1.7.3 Network Communication, Ports, Protocols and Services Report
 - 1.7.4 Control System Inventory Reports
 - 1.7.5 Software and Configuration Backups
 - 1.7.6 Cybersecurity Network (Riser) Diagram
 - 1.7.7 STIG, SRG and Vendor Guide Compliance Result Report
 - 1.7.8 Control System Cybersecurity Documentation

- 1.7.8.1 Software Applications
- 1.7.8.2 For HVAC Control System Devices
 - 1.7.8.2.1 HVAC Control System Devices FULLY Supporting User Accounts
 - 1.7.8.2.2 All Other HVAC Control System Devices
- 1.8 SOFTWARE LICENSING
- 1.9 CYBERSECURITY DURING CONSTRUCTION
 - 1.9.1 Contractor Computer Equipment
 - 1.9.1.1 Operating System
 - 1.9.1.2 Anti-Malware Software
 - 1.9.1.3 Passwords and Passphrases
 - 1.9.1.4 User-Based Authentication
 - 1.9.1.5 Demonstration of Compliance
 - 1.9.1.6 Contractor Computer Cybersecurity Compliance Statements
 - 1.9.2 Temporary IP Networks
 - 1.9.2.1 Network Boundaries and Connections
 - 1.9.3 Government Access to Network
 - 1.9.4 Temporary Wireless IP Networks
 - 1.9.5 Passwords and Passphrases
 - 1.9.6 Contractor Temporary Network Cybersecurity Compliance Statements
- 1.10 CYBERSECURITY DURING WARRANTY PERIOD

PART 2 PRODUCTS

- 2.1 ETHERNET SWITCH
 - 2.1.1 Required Functionality
 - 2.1.2 Configuration Requirements
- 2.2 DAISY CHAIN IP CONTROLLERS

PART 3 EXECUTION

- 3.1 CYBERSECURITY HARDENING AND CONFIGURATION GUIDES
- 3.2 NETWORK REQUIREMENTS
 - 3.2.1 Wireless and Wired Broadcast Communication
 - 3.2.1.1 Wireless and Wired Broadcast IP Communications
 - 3.2.1.2 Non-IP Wireless Communication
 - 3.2.1.3 Wireless and Wired Broadcast Communication Request
 - 3.2.2 Non-IP Control Networks
 - 3.2.3 IP Control Networks
 - 3.2.3.1 IP Network Routers
 - 3.2.3.2 IP Devices With Multiple Ethernet Connections
 - 3.2.4 Cryptographic Protection
 - 3.2.5 Device Identification and Authentication
 - 3.2.5.1 For HVAC Control System Devices
 - 3.2.6 Cryptographic Module Authentication
- 3.3 ACCESS CONTROL REQUIREMENTS
 - 3.3.1 User Accounts
 - 3.3.1.1 Computers
 - 3.3.1.2 Controllers
 - 3.3.1.2.1 HVAC Control Systems
 - 3.3.2 Unsuccessful Logon Attempts
 - 3.3.2.1 Devices MINIMALLY Supporting Accounts
 - 3.3.2.2 Devices FULLY Supporting Accounts
 - 3.3.3 System Use Notification
 - 3.3.3.1 System Use Notification for Remote User Interfaces
 - 3.3.3.2 System Use Notification for Local User Interfaces
 - 3.3.4 Permitted Actions Without Identification or Authentication
- 3.4 USER IDENTIFICATION AND AUTHENTICATION
 - 3.4.1 User Identification and Authentication for All System Types
 - 3.4.2 User Identification and Authentication for Specific System Types

- 3.4.2.1 HVAC Control Systems Devices
- 3.4.3 User Identification and Authentication for Specific Devices
- 3.4.4 Implementation of Identification and Authorization Requirements
- 3.4.5 Password-Based Authentication Requirements
 - 3.4.5.1 Passwords for Software and Applications Running on Computers
 - 3.4.5.2 Passwords for Controllers FULLY Supporting Accounts
 - 3.4.5.3 Passwords for Remote Interfaces
 - 3.4.5.4 Passwords for Devices Minimally Supporting Accounts
- 3.4.6 Authenticator Feedback
- 3.5 CYBERSECURITY AUDITING
 - 3.5.1 Audit Events, Content of Audit Records, and Audit Generation
 - 3.5.1.1 Computers
 - 3.5.1.1.1 Audited Events
 - 3.5.1.1.2 Audit Event Information To Record
 - 3.5.1.2 For HVAC Control System Controllers
 - 3.5.1.2.1 HVAC Control System Controllers FULLY Supporting User Accounts
 - 3.5.1.2.1.1 Audited Events
 - 3.5.1.2.1.2 Audit Event Information To Record
 - 3.5.1.2.2 Other HVAC Control System Controllers
 - 3.5.2 Audit Time Stamps
 - 3.5.3 Auditing Front End Software
 - 3.5.3.1 Import and Upload Requirements
 - 3.5.3.2 Export Requirements
 - 3.5.4 Audit Storage Capacity and Audit Upload
 - 3.5.4.1 Device Audit Record Upload Software
 - 3.5.5 Response to Audit Processing Failures
- 3.6 REQUIREMENTS FOR LEAST FUNCTIONALITY
 - 3.6.1 Device Capabilities
 - 3.6.2 Software
- 3.7 SYSTEM AND COMMUNICATION PROTECTION
 - 3.7.1 Collaborative Computing
 - 3.7.2 Denial of Service Protection
- 3.8 SAFE MODE AND FAIL SAFE OPERATION
- 3.9 SYSTEM MAINTENANCE TOOL SOFTWARE
- 3.10 DEVICE POWER
- 3.11 VULNERABILITY SCANNING
 - 3.11.1 Computers and Software Running on Computers
 - 3.11.2 Controllers
- 3.12 FIPS 201-2 REQUIREMENT
- 3.13 SYSTEM AND INTEGRATION INTEGRITY
 - 3.13.1 Malicious Code Protection
- 3.14 CONTROL SYSTEM CYBERSECURITY TESTING
 - 3.14.1 Control System Cybersecurity Testing Procedures
 - 3.14.2 Control System Cybersecurity Testing Execution
 - 3.14.3 Control System Cybersecurity Testing Report
- 3.15 FIELD QUALITY CONTROL, CYBERSECURITY VALIDATION SUPPORT
- 3.16 CYBERSECURITY TRAINING

AM0003*

*AM0003

-- End of Section Table of Contents --

SECTION 25 05 11.01

CYBERSECURITY FOR FACILITY-RELATED CONTROL SYSTEMS: HVAC

PART 1 GENERAL

Many subparts in this Section contain text in curly braces ("{" and "}") indicating which cybersecurity control and control correlation identifier (CCI) the requirements of the subpart relate to. The text inside these curly braces is for Government reference only and enables coordination of the requirements of this Section with the RMF process throughout the design and construction process. Text in curly braces are not contractor requirements.

This Section refers to Security Requirements Guide (SRGs) and Security Technical Implementation Guide (STIGs). STIGs and SRGs are available online at the Information Assurance Support Environment (IASE) website at <https://public.cyber.mil/stigs/downloads/> and an SRG/STIG Applicability Guide and Collection Tool is available at <https://public.cyber.mil/stigs/SCAP/>. Not all control system components have applicable STIGs or SRGs. The "Control Systems SRG" does not apply to work performed under this Section; all requirements within this section to apply applicable SRGs DO NOT include the "Control Systems SRG".

1.1 CONTROL SYSTEM APPLICABILITY

There are multiple versions of this Section associated with this project. Different versions have requirements applicable to different control systems. This specific Section applies only to the following control systems: HVAC.

1.2 RELATED REQUIREMENTS

This section does not contain sufficient requirements to procure a control system and must be used in conjunction with other Sections which specify control systems. This Section adds cybersecurity requirements to the control systems specified in other Sections, and as these requirements are conditioned on the control system being provided, there may be requirements in this Section that will not apply to this project. All Sections containing facility-related control systems or control system components are related to the requirements of this Section. Review all specification sections to determine related requirements.

In cases where a requirement is specified in both this Section and in another Section, the more stringent requirement must be met. In cases where a requirement in this Section conflicts with the requirements of another Section such that both requirements cannot be met at the same time, request direction from the Contracting Officer to determine which requirement applies to the project.

1.3 REFERENCES

The publications listed below form a part of this specification to the extent referenced. The publications are referred to within the text by the basic designation only.

AMERICAN SOCIETY OF HEATING, REFRIGERATING AND AIR-CONDITIONING
ENGINEERS (ASHRAE)

ASHRAE 135

(2020; Interpretation 1-8 2021; Errata 1-2 2021; Addenda CD 2021; Addenda BV-CE 2022; Interpretation 9-12 2022; Interpretation 13-24 2023; Addenda BV-CF 2023; Errata 3 2023) BACnet—A Data Communication Protocol for Building Automation and Control Networks

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS (IEEE)

IEEE 802.1x (2010) Local and Metropolitan Area Networks - Port Based Network Access Control

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

NIST FIPS 140-2 (2001) Security Requirements for Cryptographic Modules

NIST FIPS 201-2 (2013) Personal Identity Verification (PIV) of Federal Employees and Contractors

U.S. DEPARTMENT OF DEFENSE (DOD)

DODI 8551.01 (2014) Ports, Protocols, and Services Management (PPSM)

DTM 08-060 (2008) Policy on Use of Department of Defense (DoD) Information Systems - Standard Consent Banner and User Agreement

1.4 DEFINITIONS

1.4.1 Administrator Account

An administrator account is an account with full permissions to a device, application, or operating system, including the ability to create and modify other user accounts.

Note that the operating system Administrator Account may be different than Administrator Accounts for applications hosted on that operating system. Also, most controllers will not have any support for accounts and will therefore not have an 'Administrator Account'.

1.4.2 Computer

A computer is one of the following:

- a. a device running a non-embedded desktop or server version of Microsoft Windows
- b. a device running a non-embedded version of MacOS
- c. a device running a non-embedded version of Linux
- d. a device running a version or derivative of the Android Operating System, where Android is considered separate from Linux
- e. a device running a version of Apple iOS

Unless otherwise indicated or clear from context use of the word "device" in this Section includes computers.

1.4.3 Controller

A device other than a computer or Ethernet switch.

1.4.4 Mission Space

A device or media is in mission space if physical access to the device or media is controlled by the organization served by the device. For example, a variable air volume (VAV) box controller in a suspended ceiling is in mission space if the VAV box serves that room; an electrical switchgear in an

electrical room or an air handling unit (AHU) in a mechanical room or on a rooftop may still be considered to be in mission space if the organization (mission) served by that switchgear or AHU controls access to the electrical room, mechanical room or rooftop.

1.4.5 Network

A network is a group of two or more devices that can communicate using a network protocol. Network protocols must provide a method for addressing devices on the network; a communication method that does not provide an addressing scheme is not a networked form of communication. Devices that communicate using a method of communication that does not support device addressing are not using a network. Addresses may be other than IP addresses, and addressing may be at either Open Systems Interconnection (OSI) layer 2 or layer 3.

1.4.6 Network Connected

A component is network connected (or "connected to a network") only when the device has a network transceiver which is directly connected to the network and implements the network protocol. A device lacking a network transceiver (and accompanying protocol implementation) can never be considered network connected. Note that (unlike many IT definitions of "Network Connected") a device connected to a non-IP network is still considered network connected (an IP connection or IP address is not required for a device to be network connected).

1.4.6.1 Wireless Network Connected

Any device that supports wireless network communication is network connected to a wireless network, regardless of whether the device is communicating using wireless. Unless physically disabled, devices with wireless transceivers support wireless, it is not sufficient to disable the wireless in software.

1.4.7 Network Media

The thing that provides the communication channel between the devices on a network. Typically wire, but might include wireless, fiber optic, or even power line (some network protocols allow sending network signals over power wiring).

1.4.8 User Account Support Levels

The support for user accounts is categorized in this Section as one of three levels:

1.4.8.1 FULLY Supported

Device supports configurable individual accounts. Accounts can be created, deleted, modified, etc. Privileges can be assigned to accounts. These devices support user-based (as opposed to role-based) authentication.

1.4.8.2 MINIMALLY Supported

Device supports a small, fixed number of accounts (perhaps only one). Accounts cannot be modified. A device with only a "User" and an "Administrator" account would fit this category. Similarly, a device with two PINs for logon - one for restricted and one for unrestricted rights would fit here (in other words, the accounts do not have to be the traditional "username and password" structure). These devices typically only support role-based authentication.

Examples of devices which MINIMALLY support accounts are a) a variable frequency drive with a single account which requires a PIN for access to configuration; and b) a room lighting control touchpad interface that has a single account.

1.4.8.3 NOT Supported

Device does not support any Access Enforcement therefore the whole concept of "account" is

meaningless.

1.4.9 Manual Local Input

Manual Local Inputs are system analog or binary inputs that are adjustable by a person but are, by intrinsic hardware design, very limited in potential capabilities. Manual Local Inputs do not have touch screens or full keyboards, but may have a few buttons or dials to allow input. Manual Local Inputs do not have full graphic screens or dot-matrix displays, but may have simple lights (LEDs) or 7-segment displays. Manual Local Inputs do not have any sort of menu structure, each button has a single well-defined function.

Examples of Manual Local Inputs are H-O-A switches, simple thermostats, and disconnect switches.

1.4.10 Card Reader

A card reader is an input/output device whose primary function is to assist in two-factor authentication. A card reader must have an interface to read data from a card and may be able to write data to a card. A card reader may have a means (such as buttons, keypad, touchscreen, etc.) for a user to input a PIN or password, as well as a limited display.

1.4.11 User Interface

A User Interface (UI) is something other than a Manual Local Input or Card Reader that allows a person to interact with the system or device. Note that while a Card Reader is not by itself a User Interface, a User Interface may contain a Card Reader in order for it to authenticate its user. Within control systems, there are a wide range of User Interfaces.

Two important distinctions are 1) whether the user interface is Local or Remote, and 2) the effective capabilities of the User Interface to alter data, which is the "privilege" of the user interface (where effective privilege available to a specific user at a specific user interface is the combination of the greatest privilege offered by the user interface and the specific account the user is logged into).

1.4.11.1 Local User Interface

A Local User Interface is a user interface where the physical hardware the user interacts with (keyboard, buttons, display, etc.) is physically part of the device being affected. All of the relevant characteristics of the user interface are embodied within a single device.

Note that a Local UI may be able to access data in a different device, Local versus Remote in this context refers to the user interface itself; the capability to access data in a different device is covered under "Full User Interface".

1.4.11.2 Remote User Interface

A Remote User Interface implements a Client/Server model where the physical hardware the user interacts with (Client) is physically distinct from the device being affected (Server). Most or all of the security and functionality characteristics of the user interface are defined by the Server, not the Client. The Client and Server communicate via a network connection. A common example of a remote user interface is a web-based interface where the browser (client) is generally on different hardware than the web server (server). A Remote UI remains a Remote UI even if the user happens to be at a Client on the same hardware as the Server. What is important is that a) the Client may be on different hardware than the Server and b) the majority of the security and functional characteristics of the interface are defined at the Server.

Note that this definition of "remote" is consistent with that generally used in the control industry but is not aligned with the NIST 800-53 definition of "Remote", which refers to "outside the system". The term "Remote" here better aligns with the NIST 800-53 definition of "Network" (remote from within the system) Access.

1.4.11.3 Types of User Interface (by capability)

User interfaces are also categorized by their capabilities as being Read Only, Limited, or Full.

1.4.11.3.1 Read-Only User Interface

A Read Only User Interface (also referred to as a View-Only User Interface) is a user interface that only allows for reading data, it does not allow (have the capability to) modify data. A Read Only User Interface may be either Local or Remote. A User Interface that is configured to be Read Only (by some other means than the interface itself, such as using configuration software on a laptop) is a Read-Only Interface. Note a Read Only User Interface may have buttons (or touch screen, etc.) allowing the user to navigate through the presentation of data.

Examples of a Read Only User Interfaces are a) a publicly viewable "energy dashboard" showing weather data and energy usage within a building and b) digital wayfinding signage.

1.4.11.3.2 Limited User Interface

A Limited User Interface is a user interface that - by design - can only alter information local to the user interface. Note that the determination of "alter" includes only direct interactions, it explicitly excludes interactions that might occur as secondary effects. For example, an interface changing the flow setpoint in a pump controller is a direct interaction, the subsequent change in flow (as well as any subsequent downstream changes in valve position) are not direct interactions.

Two examples of LIMITED UIs are: a) a variable speed drive has a Limited Local User Interface which allows the user to change properties within the drive, but does not allow affecting things outside the drive; and b) a typical home WiFi Router has a Limited Remote User Interface which allows configuration of the Router, but does not allow direct interaction with other devices.

1.4.11.3.3 Full User Interface

A Full User Interface can alter information in devices outside the device with the user interface. For example, a typical Local Display Panel is a Full Local User Interface while a browser-based front end is a Full Remote User Interface.

1.4.11.3.4 View-Only User Interface

See Read-Only User Interface

1.4.11.4 Other User Interface Terminology

In addition to defining whether a user interface is a Hardware Limited, Read-Only, Limited or Full, and whether it is Local or Remote, user interfaces are classified by whether they are writable or privileged.

1.4.11.4.1 Writable User Interface

Any User Interface that is not Read-Only is Writable. (Limited User Interfaces and Full User Interfaces are both writable user interfaces (as they are capable of changing a value)).

1.4.11.4.2 Privileged User Interface

A Privileged UI is a UI that has sufficient capabilities or functionality that it requires specific cybersecurity measures to be put in place to limit its unauthorized use. Ultimately, whether a specific user interface is considered a Privileged User Interface must be determined by usage. Unless otherwise specified, user interfaces can be determined to be privileged or not using the following:

- a. Read-Only User Interfaces are not privileged user interfaces.
- b. Full User Interfaces are privileged user interfaces.

- c. User interfaces that allow for configuration of auditing or allows for modification or deletion of audit logs are privileged user interface.
- d. User interfaces that allow for reprogramming a network connected device is a privileged user interface.
- e. Except as specified above, a Limited User Interface must be determined to be privileged or not based on the specific capabilities and use case of the user interface. In general however, user interfaces that do not offer significant capabilities above and beyond those available at that location via other means (e.g. such as a disconnect switch, breaker, or hand-off-auto switch, or physical attack) are not privileged.

1.4.12 Wireless Network

Any network that communicates without using wires or fiber optics as the communication media. Wireless networks include: WiFi, Bluetooth, ZigBee, cellular, satellite, long and short wave radio, 2.4 GHz, free space optical, point-to-point laser, microwave, and IR.

1.4.13 Wired Broadcast Network

Wired Broadcast Networks are any network, such as powerline carrier networks and modem (wired telephony), that use wire-based technologies where there is not a clearly defined boundary for signal propagation.

1.5 ADMINISTRATIVE REQUIREMENTS

1.5.1 Points of Contact

Coordinate with the following Points of Contact as indicated in this Section and as required. Not all projects will require coordination with all Points of Contact. When coordination is required and no Point of Contact is indicated, coordinate with the Contracting Officer (KO).

- a. Government Computer Access Point of Contact: Contracting Office (KO)
- b. HTTPS Certificate Point of Contact: Contracting Officer (KO)
- c. Email Address Point of Contact: Contracting Officer (KO)
- d. Password Point of Contact: Contracting Officer (KO)
- e. Mobile Code Point of Contact: Contracting Officer (KO)

1.5.2 Coordination

Coordinate the execution of this Section with the execution of all other Sections related to control systems as indicated in the paragraph RELATED REQUIREMENTS. Items that must be considered when coordinating project efforts include but are not limited to:

- a. If requesting permission for wireless or wired broadcast communication, the Wireless and Wired Broadcast Communication Request submittal must be approved prior to control system device selection and installation.
- b. If requesting permission for alternate account lock permissions, the Device Account Lock Exception Request must be approved prior to control system device selection and installation.
- c. If requesting permission for the use of a device with multiple physical connections to IP networks, the Multiple IP Connection Device Request must be approved prior to control system device selection and installation.

- d. Wireless testing may be required as part of the control system testing. See requirements for the Wireless Communication Test Report submittal.
- e. If the Device Audit Record Upload Software is to be installed on a computer not being provided as part of the control system, coordination is required to identify the computer on which to install the software.
- f. The Cybersecurity Interconnection Schedule must be coordinated with other work that will be interconnected to, and interconnections must be approved by the Government before relying on them for system functionality.
- g. Cybersecurity testing support must be coordinated across control systems and with the Government cybersecurity testing schedule.
- h. Passwords must be coordinated with the indicated contact for the project site.
- i. If applicable, HTTPS web server certificates must be obtained from the indicated HTTPS Certificate Point of Contact.
- j. Contractor Computer Cybersecurity Compliance Statements must be provided for each contractor using contractor owned computers.

1.6 SUBMITTALS

Government approval is required for submittals with a "G" or "S" classification. Submittals not having a "G" or "S" classification are for information only. When used, a code following the "G" classification identifies the office that will review the submittal for the Government. Submit the following in accordance with Section 01 33 00 SUBMITTAL PROCEDURES:

SD-01 Preconstruction Submittals

Wireless and Wired Broadcast Communication Request; G

Device Account Lock Exception Request; G

Multiple Ethernet Connection Device Request; G

Contractor Computer Cybersecurity Compliance Statements; G

Contractor Temporary Network Cybersecurity Compliance Statements; G

Cybersecurity Interconnection Schedule; G

Proposed STIG and SRG Applicability Report; G

Pre-Construction Control System Inventory Report; G

SD-02 Shop Drawings

Network Communication, Ports, Protocols and Services Report; G

Cybersecurity Network (Riser) Diagram; G

SD-03 Product Data

Control System Cybersecurity Documentation; G

SD-06 Test Reports

Control System Cybersecurity Testing Procedures; G

Control System Cybersecurity Testing Report; G

SD-07 Certificates

Software Licenses; G

SD-11 Closeout Submittals

Software and Configuration Backups; G

Auditing Front End Software; G

Device Audit Record Upload Software; G

System Maintenance Tool Software; G

Control System Scanning Tools; G

STIG, SRG and Vendor Guide Compliance Result Report; G

Final Control System Inventory Report; G

1.7 CYBERSECURITY DOCUMENTATION

{For Government Reference Only: This subpart (and its subparts) relates to PL-7; CCI-003071}

1.7.1 Proposed STIG and SRG Applicability Report

For each model of network connected or network infrastructure device, use the DISA SRG/STIG Applicability Guide and Collection Tool (available at <https://public.cyber.mil/stigs/SCAP/>) to identify applicable STIGs or SRGs and provide a report indicating applicable STIGs and SRGs for each model. Provide the Proposed STIG and SRG Applicability Report concurrently with the Pre-Construction Control System Inventory Report.

1.7.2 Cybersecurity Interconnection Schedule

{For Government Reference Only: This subpart relates to CA-3(b), PL-8, SC-7(9), SC-7(11); CCI-000258, CCI-003072, CCI-003073, CCI-003075, CCI-002398, CCI-002399, CCI-002401, CCI-002402, CCI-002403.}

Provide a completed Cybersecurity Interconnection Schedule documenting network connections between the installed system and other systems. Provide the following information for each device directly communicating between systems: Device Identifier, Device Manufacturer, Device Description, Transport layer Protocol, Network Address, Port (if applicable), MAC (Layer 2) address (if applicable), Media, Application Protocol, Service (if applicable), Descriptive Purpose of communication. If other control system Sections used on this project include submittals documenting this information, provide copies of those submittals to meet this requirement.

In addition to the requirements of Section 01 33 00 SUBMITTAL PROCEDURES, provide the Cybersecurity Interconnection Schedule as an editable Microsoft Excel file (a template Cybersecurity Interconnection Schedule in Excel format is available at <https://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-25-05-11>.)

1.7.3 Network Communication, Ports, Protocols and Services Report

{For Government Reference Only: This subpart (and its subparts) relates to CA-9, PL-8; CCI-002102,

CCI-002103, CCI-002104, CCI-002105, CCI-003072, CCI-003073, CCI-003075 and also the submittal requirements associated with CM-6, CM-7, including CM-7(3), CCI-000388.}

Provide a Network Communication, Ports, Protocols and Services Report. For each networked device, document device identifier and the communication characteristics of the device including communication protocols, services used, encryption employed, and a general description of what information is communicated over the network. For each device using IP communication, document all TCP and UDP ports used. For each device using non-IP communication, document communication protocol and media used. If other control system Sections used on this project include submittals documenting this information, provide copies of those submittals to meet this requirement.

In addition to the requirements of Section 01 33 00 SUBMITTAL PROCEDURES, provide the Network Communication, Ports, Protocols and Services Report as an editable Microsoft Excel file.

1.7.4 Control System Inventory Reports

{For Government Reference Only: This subpart (and its subparts) relates to CM-8(a), SI-17, IA-3; CCI-000389, CCI-000392, CCI-000398, CCI-002773, CCI-002774, CCI-002775, CCI-000777, CCI-000778, CCI-001958}

Provide a [Pre-Construction Control System Inventory Report](#) report and a [Final Control System Inventory Report](#), using the Inventory Spreadsheet listed under this Section at <https://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-25-05-11>. In the Control System Inventory Reports, document all devices, including networked devices, network infrastructure devices, non-networked devices, input devices (e.g. sensors) and output devices (e.g. actuators). For each device provide all applicable information for which there is a field on the spreadsheet in accordance with the instructions on the spreadsheet.

In addition to the requirements of Section 01 33 00 SUBMITTAL PROCEDURES, provide the Control System Inventory Reports as editable Microsoft Excel files. Provide the Pre-Construction Control System Inventory Report concurrently with the Proposed STIG and SRG Applicability Report

1.7.5 Software and Configuration Backups

{For Government Reference Only: This subpart (and its subparts) relates to CP-10; CCI-000550, CCI-000551, CCI-000552}

For each computer on which software is installed under this project, provide a recovery image of the final as-built computer. This image must allow for bare-metal restore such that restoration of the image is sufficient to restore system operation to the imaged state without the need for re-installation of software. If additional user permissions are required to meet this requirement, coordinate the creation of the image with the identified Government Computer Access Point of Contact.

For all Ethernet switches provide a backup of the switch configuration. For all controllers, provide a backup of the controller configuration and the source code for all loaded application programs (all software that is not common to every controller of the same manufacturer and model).

If any or all of these are provided under another Section, provide documentation indicating this and referencing those submittals.

1.7.6 Cybersecurity Network (Riser) Diagram

{For Government Reference Only: This subpart (and its subparts) relates to PL-2(a), PL-8; CCI-003051, CCI-003053, CCI-003072, CCI-003073, CCI-003075}

Provide a cybersecurity network (riser) diagram of the complete control system including all network and device hardware. For each device, include the device identifier, device type, and manufacturer. If

the control system specifications require a riser diagram submittal, provide a copy of that submittal as the cybersecurity riser diagram. Otherwise, provide a riser diagram in one-line format.

1.7.7 STIG, SRG and Vendor Guide Compliance Result Report

For every component (device or software) with an applicable STIG or SRG in the Proposed STIG and SRG Applicability Report, document compliance with the STIG or SRG requirements.

- a. For components which are scannable by the Evaluate-STIG tool (available online at [\(CAC Required\)](#)), include the Evaluate-STIG report and raw scan results in addition to the final, manually reviewed and revised, documentation of compliance with STIG and SRG requirements. Checklist files should not contain any findings with a Not Reviewed (NR) status after manual reviews.
- b. For components which do not support automated scanning, a manual review using the General Purpose STIG option should be done. A completed Checklist file should not contain any findings with a Not Reviewed (NR) status after manual reviews

For every component (device or software) with manufacturer provided cybersecurity documentation, procedure, or method for secure configuration or installation, provide a report documenting how the component was configured and any deviation from the manufacturer instructions.

1.7.8 Control System Cybersecurity Documentation

{For Government Reference Only: This subpart (and its subparts) relates to SA-5(a),SA-5(b),SA-5(c), SA-22(b); CCI-003124, CCI-003125, CCI-003126, CCI-003127, CCI-003128, CCI-003129, CCI-003130, CCI-003131, CCI-003374}

Provide a Control System Cybersecurity Documentation submittal containing the indicated information for each device and software application.

1.7.8.1 Software Applications

For all software applications running on computers provide:

- a. administrator documentation that describes secure configuration of the software {For Government Reference Only: relates to CCI-003124}
- b. administrator documentation that describes secure installation of the software and software updates. {For Government Reference Only: relates to CCI-003125}
- c. administrator documentation that describes secure operation of the software {For Government Reference Only: relates to CCI-003124}
- d. administrator documentation that describes effective use and maintenance of security functions or mechanisms for the software {For Government Reference Only: relates to CCI-003127}
- e. administrator documentation that describes known vulnerabilities regarding configuration and use of administrative (i.e. privileged) functions for the software {For Government Reference Only: relates to CCI-003128}
- f. user documentation that describes user-accessible security functions or mechanisms in the software and how to effectively use those security functions or mechanisms {For Government Reference Only: relates to CCI-003129}
- g. user documentation that describes methods for user interaction which enables individuals to use the software in a more secure manner {For Government Reference Only: relates to CCI-003130}

- h. user documentation that describes user responsibilities in maintaining the security of the software
{For Government Reference Only: relates to CCI-003131}

1.7.8.2 For HVAC Control System Devices

1.7.8.2.1 HVAC Control System Devices FULLY Supporting User Accounts

For all HVAC Control System Devices which FULLY support user accounts, provide:

- a. Documentation that describes secure configuration of the device {For Government Reference Only: relates to CCI-003124}
- b. Documentation that describes secure operation of the device {For Government Reference Only: relates to CCI-003124}
- c. Documentation that describes effective use and maintenance of security functions or mechanisms for the device {For Government Reference Only: relates to CCI-003127}
- d. Documentation that describes known vulnerabilities regarding configuration and use of administrative (i.e. privileged) functions for the device {For Government Reference Only: relates to CCI-003128}
- e. Documentation that describes user-accessible security functions or mechanisms in the device and how to effectively use those security functions or mechanisms; or a specific indication that there are no user-accessible security functions or mechanisms in the device {For Government Reference Only: relates to CCI-003129}
- f. Documentation that describes methods for user interaction which enables individuals to use the device in a more secure manner {For Government Reference Only: relates to CCI-003130}

1.7.8.2.2 All Other HVAC Control System Devices

For all HVAC Control System Devices which do not FULLY support user accounts, provide:

- a. Documentation that describes secure configuration of the device; or a specific indication that there are no secure configuration steps that apply {For Government Reference Only: relates to CCI-003124}
- b. Documentation that describes effective use and maintenance of security functions or mechanisms for the device; or a specific indication that there are no security functions or mechanisms in the device {For Government Reference Only: relates to CCI-003127}
- c. For devices which include a user interface, documentation that describes methods for user interaction which enables individuals to use the device in a more secure manner {For Government Reference Only: relates to CCI-003130}

1.8 SOFTWARE LICENSING

{For Government Reference Only: This subpart (and its subparts) relates to SI-2(a), SI-2(c), SI-7(14); CCI-001227, CCI-002605, CCI-002737}

For all software provided that has not already been licensed to the government or project site, provide a license to the project site for a period of no less than 5 years, and the license must also include the following software updates:

- a. Security and bug-fix patches issued by the software manufacturer.
- b. Security patches to address any vulnerability identified in the National Vulnerability Database at <http://nvd.nist.gov> with a Common Vulnerability Scoring System (CVSS) severity rating of

MEDIUM or higher.

Provide a single [Software Licenses](#) submittal with documentation of the software licenses for all software provided

1.9 CYBERSECURITY DURING CONSTRUCTION

{For Government Reference Only: This subpart (and its subparts) relates to AC-18, CA-3; CCI-000258}

In addition to the control system cybersecurity requirements indicated in this section, meet following requirement throughout the construction process.

1.9.1 Contractor Computer Equipment

Contractor owned computers may be used for construction. Contractor computers connected to the control system, control system network, or a control system component at any point during construction must meet the following requirements:

1.9.1.1 Operating System

The operating system must be an operating system currently supported by the manufacturer of the operating system. The operating system must be current on security patches and operating system manufacturer required updates.

1.9.1.2 Anti-Malware Software

The computer must run anti-malware software from a reputable software manufacturer. Anti-malware software must be a version currently supported by the software manufacturer, must be current on all patches and updates, and must use the latest definitions file. Computers used on this project must perform a full antivirus scan at least once per day. Computers which have connected to any other network since the last full antivirus scan must perform a full antivirus scan prior to connection to the control system network or to the temporary contractor-installed IP network. Perform an antivirus scan on all removable media (e.g., external hard drives, CDs, DVDs, USB flash drives) prior to connecting to the control system environment.

1.9.1.3 Passwords and Passphrases

The passwords and passphrases for computers, applications, and web-based applications supporting passwords must be changed from their default values. Passwords must be a minimum of eight characters with a minimum of one uppercase letter, one lowercase letter, one number and one special character.

1.9.1.4 User-Based Authentication

Each user must have a unique account; sharing of a single account between multiple users is prohibited.

1.9.1.5 Demonstration of Compliance

The Government has the right to require demonstration of computer compliance with these requirements at any time during the project.

1.9.1.6 [Contractor Computer Cybersecurity Compliance Statements](#)

Provide a single submittal containing completed Contractor Computer Cybersecurity Compliance Statements for each company using contractor owned computers. Contractor Computer Cybersecurity Compliance Statements must use the template published at <https://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-25-05-11>. Each Statement must be signed by a cybersecurity

representative for the relevant company.

1.9.2 Temporary IP Networks

Temporary contractor-installed IP networks may be used during construction. When used, temporary contractor-installed IP networks connected to the control system, control system network, or a control system component at any point during construction must meet the following requirements:

1.9.2.1 Network Boundaries and Connections

The network must not extend outside the project site and must not connect to any IP network other than those specifically provided or furnished for this project. Any and all access to the network from outside the project site is prohibited.

1.9.3 Government Access to Network

Government personnel must be allowed to have complete and immediate access to the network at any time in order to verify compliance with this specification.

1.9.4 Temporary Wireless IP Networks

In addition to the other requirements on temporary IP networks, temporary wireless IP (WiFi) networks, when permitted, must not interfere with existing wireless networks, must use WPA2 security and must not broadcast the network name (SSID). Network names (SSID) for wireless networks must be changed from their default values.

1.9.5 Passwords and Passphrases

The passwords and passphrases for all network devices and network access must be changed from their default values. Passwords must be a minimum 8 characters with a minimum of one uppercase letter, one lowercase letter, one number and one special character.

1.9.6 Contractor Temporary Network Cybersecurity Compliance Statements

Provide a single submittal containing completed Contractor Temporary Network Cybersecurity Compliance Statements for each company implementing a temporary IP network. Contractor Temporary Network Cybersecurity Compliance Statements must use the template published at <https://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-25-05-11>. Each Statement must be signed by a cybersecurity representative for the relevant company. If no temporary IP networks will be used, provide a single copy of the Statement indicating this.

1.10 CYBERSECURITY DURING WARRANTY PERIOD

All work performed on the control system after acceptance must be performed using Government Furnished Equipment or equipment specifically and individually approved by the Government.

PART 2 PRODUCTS

All products used on this project must meet the indicated requirements, but not all products specified here will be required by every project.

2.1 ETHERNET SWITCH

Provide Open Systems Interconnection (OSI) Layer 2 Ethernet switches with the following capabilities, and with an interface to support switch configuration for these capabilities:

2.1.1 Required Functionality

Switches must:

- a. Copper Ethernet ports must auto negotiate for 10, 100 and 1000 megabits-per-second links.
- b. Be capable of implementing port level access control by MAC address and limit the number of MAC addresses to one MAC address per port.
- c. For LOW Impact Systems, be capable of implementing per-port access control lists (ACLs) where the list can be filtered by source and destination IP addresses, and by source and destination UDP or TCP ports.

2.1.2 Configuration Requirements

Switches must:

- a. Support configuration save and restore.
- b. Support both manual IP address assignment and acquisition of a dynamic IP address via Dynamic Host Configuration Protocol (DHCP).
- c. Be capable of limiting access for configuration to one or more of: a web interface using HTTPS, a command line interface using SSH, or an SNMP connection using SNMP version 3 or later.
- d. Support the ability to lock configuration capability to a dedicated management port.

2.2 DAISY CHAIN IP CONTROLLERS

Controllers used as Daisy Chain IP Controllers must be IP controllers with exactly two Ethernet network connections and basic built-in switch capabilities to allow implementation of an Ethernet network in a daisy chain architecture. Switches incorporated by Daisy Chain IP Controllers are not required to meet the requirements for Ethernet Switches as defined in this Section.

PART 3 EXECUTION

3.1 CYBERSECURITY HARDENING AND CONFIGURATION GUIDES

Install, configure, and harden all hardware and software furnished on this project in accordance with manufacturer provided documentation, procedures, or methods for secure configuration or installation. Do not implement specific hardening actions if that action would conflict with required functionality or another requirement of this Section.

3.2 NETWORK REQUIREMENTS

3.2.1 Wireless and Wired Broadcast Communication

{For Government Reference Only: This subpart (and its subparts) relates to AC-18, AC-18(3); CCI-001438, CCI-001439, CCI-002323, CCI-001441, CCI-001449}

Unless explicitly authorized by the Government, do not use any wireless or wired broadcast communication.

3.2.1.1 Wireless and Wired Broadcast IP Communications

Do not install wireless or wired broadcast IP networks, including: do not install a wireless access point; do not install or configure an ad-hoc wireless network; do not install or configure a WiFi Direct communication.

When explicitly authorized by the Government, wireless IP communication may be used to communicate with an existing wireless network.

3.2.1.2 Non-IP Wireless Communication

For LOW Impact Systems: When non-IP wireless communication is explicitly authorized by the Government, use the maximum level of encryption supported by the specific protocol employed and select signal strength and radiated power to the minimum necessary for reliable communication.

3.2.1.3 Wireless and Wired Broadcast Communication Request

Provide a report documenting the proposed use of wireless or wired broadcast communication prior to device selection using the Wireless and Wired Broadcast Communication Request Schedule at <https://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-25-05-11>. If there is no proposed use of wireless or wired broadcast communication, provide a document indicating this instead of the Request Schedule.

For each device proposed to use wireless or wired broadcast communication show: the device identifier, a description of the device, the location of the device, the device identifiers of other devices communicating with the device, the protocol used for communication, encryption type and strength. For wireless communication, also show: RF Frequency, Radiated Power in dBm (decibel with a milliwatt reference), free-space range, and the expected as-installed range.

3.2.2 Non-IP Control Networks

When control system specifications require particular communication protocols, use only those communication protocols and only as specified. Do not implement any other communication protocol.

When control system specifications do not indicate requirements for communication protocols, use only those protocols required for operation of the system as specified.

3.2.3 IP Control Networks

{For Government Reference Only: This subpart relates to CM-6(a), CM-7(a), CM-7(b), CM-7(1)(b), SC-41; CCI-001588, CCI-000381, CCI-000380, CCI-000381, CCI-000382, CCI-001761, CCI-001762, CCI-002544, CCI-002545, CCI-002546.}

IP Networks must be Ethernet networks and must use switches which are Ethernet Switches or Daisy Chain IP Controllers as defined in this Section. Do not use nonsecure functions, ports, protocols and services as defined in **DDI 8551.01** unless those ports, protocols and services are specifically required by the control system specifications or otherwise specifically authorized by the Government. Do not use ports, protocols and services that are not specified in the control system specifications or required for operation of the control system.

3.2.3.1 IP Network Routers

Do not install any device that performs IP routing.

3.2.3.2 IP Devices With Multiple Ethernet Connections

Except for Ethernet Switches and Daisy Chain IP Controllers, devices must not have more than one Ethernet connection to IP networks unless doing so is required by the project specifications and the specific application is approved. If a device with Multiple Ethernet Connections to IP networks is required, provide a [Multiple Ethernet Connection Device Request](#) using the Multiple Ethernet Connection Device Request Template at <https://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-25-05-11> to request approval for each device. If a device with Multiple Ethernet Connections to IP networks is not required, instead provide a document stating that no approval is being requested.

3.2.4 Cryptographic Protection

{For Government Reference Only: This subpart relates to IA-2(9), IA-3(1), SC-8, SC-13, SC-23(1), SC-23(3); CCI-001942, CCI-001959, CCI-001967, CCI-002418, CCI-002449, CCI-002450, CCI-001185, CCI-001188, CCI-001664.}

All remote user interfaces must use HTTPS for all traffic between the user interface client and user interface server.

For devices that have STIG/SRGs related to cryptographic protection (CCI-002450), comply with the requirements of those STIG/SRGs. Ensure that all network traffic is encrypted using NSA-approved cryptography; provision of digital signatures and hashing, and FIPS-validated cryptography.

3.2.5 Device Identification and Authentication

{For Government Reference Only: This subpart (and its subparts) relates to IA-3; CCI-000777, CCI-000778, CCI-001958.}

All computers must support and implement [IEEE 802.1x](#) for device authentication to the network.

3.2.5.1 For HVAC Control System Devices

Devices using HTTP as a control protocol must use HTTPS instead. Devices using BACnet must support network security as specified for BACnet Secure Connect in [ASHRAE 135](#).

3.2.6 Cryptographic Module Authentication

{For Government Reference Only: This subpart (and its subparts) relates to IA-7; CCI-000803}

For devices (including but not limited to [NIST FIPS 140-2](#) compliant radios) that have STIG/SRGs related to cryptographic module authentication (CCI-000803), comply with the requirements of those STIG/SRGs.

3.3 ACCESS CONTROL REQUIREMENTS

3.3.1 User Accounts

{For Government Reference Only: This subpart (and its subparts) relate to AC-2(a), AC-3, AC-6(1), AC-6(10), AC-6(2), AC-6(9), CM-11(2), and IA-2; CCI-002110, CCI-000213, CCI-001558, CCI-002221, CCI-002222, CCI-002223, CCI-002235, CCI-000039, CCI-001419, CCI-002234, CCI-001812, and CCI-000764.}

Any user interface supporting user accounts (either FULLY or MINIMALLY) must limit access according to specified limitations for each account. Install and configure any device having a STIG or SRG in accordance with that STIG or SRG.

All user interfaces FULLY supporting accounts must implement user-based authentication where each account is uniquely assigned to a specific user. User interfaces FULLY supporting accounts must implement at least three (3) levels of user account privilege including: 1) an account with read-only permissions 2) an account with full permissions including account creation and modification and 3) an account with greater permissions than read-only but without account creation and modification. Disable any unnecessary or unused accounts. Disable any "guest-level" accounts that are created on the system by default.

3.3.1.1 Computers

All computer operating systems must FULLY support user accounts and implement accounts for access. Each control system software application not supporting accounts and running on a computer must be installed such that use of the software is restricted by the computer operating system to

specific users.

Applications running on computers must not require the user be logged in to a computer operating system administrator account for normal operation. It is permissible to require the computer operating system administrator account for initial application installation and configuration.

3.3.1.2 Controllers

For user interfaces provided by controllers, provide access control in accordance with the User Interface Requirements table for the applicable control system and user interface type.

- a. For table entries of "NA": NA means Not Applicable, there are no interfaces in this category.
- b. For table entries of "None Required": The user interface is not required to support user accounts.
- c. For table entries of "MINIMALLY": The user interface must at least MINIMALLY support user accounts.
- d. For table entries of "FULLY": The user interface must at FULLY support user accounts.
- e. For table entries of "KEY": The user interface must have physical security in the form of either a key lock on the interface itself or be furnished inside a lockable enclosure. Where this is required for a read only interface, the lockable enclosure must prevent viewing of data on the interface; for other interfaces, this lockable enclosure must prevent using the interface to alter data.
- f. For table entries of "Physical Security": For Local FULL interfaces, the interface must be located inside mission space. For Local Limited (not FULL) interfaces, the user interface must either a) be located within mission space or b) be protected by physical security at least as good as the control devices (and equipment controlled by the control devices) affected by the interface. For purposes of this requirement, 'affected' includes controllers with data that can be directly altered by the interface, as well as mechanical and/or electrical equipment directly controlled by those controllers, but does not include other interactions.
- g. Entries of the form "X and Y" must meet both the requirement indicated for X and the requirement indicated for Y. For example, an entry of "MINIMALLY and Physical Security" indicates the user interface must both MINIMALLY support accounts and have physical security.
- h. Entries of the form "X or Y" must meet either the requirement indicated for X or the requirement indicated for Y.

3.3.1.2.1 HVAC Control Systems

User Interface Requirements for LOW Impact HVAC Control Systems	
<u>User Interface Type</u>	<u>Access Control Requirement</u>
Local Read Only (see note 1)	None Required
Local Limited, Non-privileged	None Required
Local Limited, Privileged	Physical Security
Local Full	MINIMALLY
Remote Read Only	None Required
Remote Limited, Non-Privileged	MINIMALLY

User Interface Requirements for LOW Impact HVAC Control Systems	
<u>User Interface Type</u>	<u>Access Control Requirement</u>
Remote Limited, Privileged AND Remote Full (see note 2)	FULLY
Notes: 1)Local Read Only User Interfaces are always Non-Privileged 2)Remote Full User Interfaces are always Privileged	

3.3.2 Unsuccessful Logon Attempts

{For Government Reference Only: This subpart (and its subparts) relate to AC-7 (a), AC-7 (b); CCI-000043, CCI-000044, CCI-001423, CCI-002236, CCI-002237, CCI-002238}

Except for high availability user interfaces indicated as exempt, devices must meet the indicated requirements for handling unsuccessful logon attempts. If a device cannot meet these requirements, document device capabilities to protect from subsequent logon attempts and propose alternate protections in a [Device Account Lock Exception Request](#) submittal. Do not implement alternate protection measures in lieu of the indicated requirements without explicit permission from the Government. If no Device Account Lock Exceptions are requested, provide a document stating that no approval is being requested as the Device Account Lock Exception Request.

3.3.2.1 Devices MINIMALLY Supporting Accounts

For LOW Impact Systems: Devices which MINIMALLY (but not FULLY) support accounts must lock the user account after five consecutive failed login attempts and must unlock the user account after 15 minutes have elapsed without an unsuccessful login attempt or by a successful login to a separate administrator account.

3.3.2.2 Devices FULLY Supporting Accounts

Devices which FULLY support accounts must meet the following requirements.

- It must lock the user account when three unsuccessful logon attempts occur within a 15 minute interval.
- Once an account is locked, the account must stay locked until unlocked by an administrator. If the account being locked is the sole administrator account on the device, the account must stay locked for 1 hour and then automatically unlock.
- Once the indicated number of unsuccessful logon attempts occurs, delay further logon prompts by 5 seconds.

3.3.3 System Use Notification

{For Government Reference Only: This subpart (and its subparts) relates to AC-8; CCI-000048, CCI-002247, CCI-002243, CCI-002244, CCI-002245, CCI-002246, CCI-000050, CCI-002248}

3.3.3.1 System Use Notification for Remote User Interfaces

Remote user interfaces must display a warning banner meeting the requirements of [DTM 08-060](#) on screen.

3.3.3.2 System Use Notification for Local User Interfaces

Devices which are connected to a network and have a local user interface must display a warning banner meeting the requirements of DTM 08-060 on the user interface screen if capable of doing so and must have a permanently affixed label with an approved banner from DTM 08-060 if unable to display the warning banner on the screen. Where it is impractical (perhaps due to device size) to affix the label to the device, affix the label to the device enclosure.

Labels must be machine printed or engraved, plastic or metal, designed for permanent installation, must use a font no smaller than 14 point, and must provide a high contrast between font and background colors.

3.3.4 Permitted Actions Without Identification or Authentication

{For Government Reference Only: This subpart (and its subparts) relates to AC-14; CCI-000061, CCI-000232}

The control system must require identification and authentication before allowing any actions by a user acting from a user interface which MINIMALLY or FULLY supports accounts.

3.4 USER IDENTIFICATION AND AUTHENTICATION

{For Government Reference Only: This subpart (and its subparts) relates to IA-2, IA-2(1), IA-2(12), IA-5 IA-5(b), IA-5(c), IA-5(e), IA-5(g), IA-5(1), IA-5(11); CCI-000764, CCI-000765, CCI-001953, CCI-001954, CCI-001544, CCI-001989, CCI-000182, CCI-001610, CCI-000192, CCI-000193, CCI-000194, CCI-000205, CCI-001619, CCI-001611, CCI-001612, CCI-001613, CCI-001614, CCI-000195, CCI-001615, CCI-000196, CCI-000197, CCI-000199, CCI-000198, CCI-001616, CCI-001617, CCI-000200, CCI-001618, CCI-002041, CCI-002002, CCI-002003. }

This subpart indicates requirements for specific methods of identification and authentication for users and user accounts. Where these requirements conflict apply the following order of precedence: 1) If present, Device Specific Requirements take precedence over any other requirements; and then 2) multifactor authentication requirements take precedence over password requirements.

3.4.1 User Identification and Authentication for All System Types

Unless otherwise indicated, all user interfaces supporting accounts (either FULLY or MINIMALLY) must implement Identification and Authorization via passwords.

For LOW Impact Systems: User interfaces provided by computer operating systems must implement multifactor authentication via PIV.

3.4.2 User Identification and Authentication for Specific System Types

System specific requirements are in addition to and supersede those indicated for all system types. When no additional requirements are indicated for a specific system type the requirements for all systems still apply to that system type.

3.4.2.1 HVAC Control Systems Devices

User Interfaces which FULLY support accounts and which run on a computer must use multifactor authentication via PIV.

3.4.3 User Identification and Authentication for Specific Devices

There are no additional device specific user interface requirements

3.4.4 Implementation of Identification and Authorization Requirements

Identification and Authorization must be met by one of the following methods:

- a. Direct implementation in the user interface.
- b. For user interfaces on a computer: inheriting the Identification and Authorization from the computer operating system, either by the operating system limiting access to specific applications by user, or by the application itself having permissions based on the user logged into the computer.
- c. For remote interfaces: an implementation shared between the remote user interface server and the remote user interface client. For example, a requirement for PIV authentication may be met on a remote user interface by a PIV reader on a web browser client which sends the authentication information via HTTPS to the remote server.

3.4.5 Password-Based Authentication Requirements

3.4.5.1 Passwords for Software and Applications Running on Computers

All software and applications running on computers supporting password-based authentication must enforce the following requirements:

- a. Minimum password length of 12 characters
- b. Password must contain at least one uppercase character.
- c. Password must contain at least one lowercase character.
- d. Password must contain at least one numeric character.
- e. Password must contain at least one special character. The list of supported special characters must include at least 4 separate characters.
- f. Password must have a minimum lifetime of 24 hours.
- g. Password must have a maximum lifetime of 60 days. When passwords expire, prompt users to change passwords. Do not lock accounts due to expired passwords.
- h. Password must differ from previous five passwords, where differ is defined as changing at least 50 percent of the characters (where location is significant, a character may be reused if it is in a different position).
- i. Passwords must be cryptographically protected during storage and transmission.

3.4.5.2 Passwords for Controllers FULLY Supporting Accounts

All controllers FULLY supporting accounts and supporting password-based authentication must enforce the following requirements:

- a. Minimum password length of 12 characters
- b. Password must contain at least one uppercase character.
- c. Password must contain at least one lowercase character.
- d. Password must contain at least one numeric character.
- e. Password must contain at least one special character. The list of supported special characters

must include at least 4 separate characters.

- f. Password must have a maximum lifetime of sixty (60) days. When passwords expire, prompt users to change passwords. Do not lock accounts due to expired passwords.
- g. Password must differ from previous five passwords, where differ is defined as changing at least 50 percent of the characters.
- h. Passwords must be cryptographically protected during storage and transmission.

3.4.5.3 Passwords for Remote Interfaces

Passwords for connecting to a Remote User Interface supporting password-based authentication must enforce the following requirements:

- a. Minimum password length of 12 characters
- b. Password must contain at least one uppercase character.
- c. Password must contain at least one lowercase character.
- d. Password must contain at least one numeric character.
- e. Password must contain at least one special character. The list of supported special characters must include at least 4 separate characters.
- f. Password must have a maximum lifetime of 60 days. When passwords expire, prompt users to change passwords. Do not lock accounts due to expired passwords.
- g. Password must differ from previous five passwords, where differ is defined as changing at least 50 percent of the characters (where location is significant, a character may be reused if it is in a different position).
- h. Passwords must be cryptographically protected during storage and transmission.

3.4.5.4 Passwords for Devices Minimally Supporting Accounts

Devices MINIMALLY supporting accounts must support passwords with a minimum length of four characters.

3.4.6 Authenticator Feedback

{For Government Reference Only: This subpart relates to IA-6; CCI-000206}

Devices must never show authentication information, including passwords, on a display. Devices that momentarily display a character as it is entered, and then obscure the character, are acceptable. For devices that have STIGs or SRGs related to obscuring of authenticator feedback (CCI-000206), comply with the requirements of those STIGS/SRGs.

3.5 CYBERSECURITY AUDITING

Where an auditing requirement exists for email notification, notify via email the application administrator and Information System Security Officer (ISSO) of the event. Coordinate with the Email Address Point of Contact for email addresses. If outgoing email is not available to the system, disable email notifications.

3.5.1 Audit Events, Content of Audit Records, and Audit Generation

{For Government Reference Only: This subpart (and its subparts) relates to AU-2(a), AU-2(c),

AU-2(d), AU-3, AU-10, AU-12, AU-14(b), AU-14(1), AU-14(2), AU-14(3), CM-5(1), SC-7 (9);
CCI-000123, CCI-001571, CCI-000125, CCI-001485, CCI-000130, CCI-000131, CCI-000132,
CCI-001230, CCI-000133, CCI-000134, CCI-001487, CCI-000166, CCI-001899, CCI-000169,
CCI-001459, CCI-000171, CCI-000172, CCI-001910, CCI-001914, CCI-001919, CCI-001464,
CCI-001462, CCI-001920, CCI-001814, CCI-002400. }

For devices that have STIG/SRGs related to audit events, content of audit records or audit generation, comply with the requirements of those STIG/SRGs.

If auditing requirements can be met using existing control system alarm or event capabilities, those existing capabilities may be used to meet these requirements.

3.5.1.1 Computers

For each computer, provide the capability to select audited events and the content of audit logs. Configure computers to audit the indicated events, and to record the indicated information for each auditable event. Send logs to a syslog server that is only accessible via accounts on the system with privileged level access.

3.5.1.1.1 Audited Events

Configure each computer to audit the following events:

- a. Successful and unsuccessful attempts to access, modify, or delete privileges, security objects, security levels, or categories of information (e.g. classification levels)
- b. Successful and unsuccessful logon attempts
- c. Successful logouts
- d. Privileged activities or other system level access
- e. Concurrent logons from different workstations
- f. Successful and unsuccessful accesses to objects
- g. Program initiations
- h. Direct access to the information system
- i. Account creations, modifications, disabling, and terminations.
- j. Kernel module load, unload, and restart

3.5.1.1.2 Audit Event Information To Record

Configure each computer to record, for each auditable event, the following information (where applicable to the event):

- a. What type of event occurred
- b. When the event occurred
- c. Where the event occurred
- d. The source of the event
- e. The outcome of the event

- f. The identity of any individuals or subjects associated with the event

3.5.1.2 For HVAC Control System Controllers

3.5.1.2.1 HVAC Control System Controllers FULLY Supporting User Accounts

For each controller which FULLY supports accounts, provide the capability to select audited events and the content of audit logs. Configure controllers to audit the indicated events, and to record the indicated information for each auditable event.

3.5.1.2.1.1 Audited Events

Configure each controller to audit the following events:

- a. Successful and unsuccessful logon attempts to the controller
- b. Successful logouts
- c. All account creations, modifications, disabling, and terminations.
- d. All controller shutdown and startup

3.5.1.2.1.2 Audit Event Information To Record

Configure each controller to record, for each auditable event, the following information (where applicable to the event):

- a. what type of event occurred
- b. when the event occurred
- c. the identity of any individuals or subjects associated with the event

3.5.1.2.2 Other HVAC Control System Controllers

There are no requirements to perform auditing at HVAC field controllers that do not FULLY support accounts.

3.5.2 Audit Time Stamps

{For Government Reference Only: This subpart (and its subparts) relates to AU-8; CCI-000159, CCI-001889, CCI-001890.}

Any device (computer or controller) generating audit records must have an internal clock capable of providing time with a resolution of one second. Clocks must not drift more than 10 seconds per day. Configure the system so that each device (computer or controller) generating audit records maintains accurate time to within 1 second. Note that if the control system specifications include requirement for clocks, the most stringent requirement applies.

3.5.3 Auditing Front End Software

The project site currently has the following software to support control system auditing: none. If there is no existing auditing front end software or the software is not compatible with the provided control systems, provide Auditing Front End Software with audit log import and upload, export, notification, and analysis functionality. The Auditing Front End Software may be provided as a component of the control system front end or as a separate software package, and a single package may serve multiple control systems provided under the same projects if they are sharing a cybersecurity authorization.

When the Auditing Front End Software is neither existing nor installed under the requirements of

another Section, furnish the Auditing Front End Software media and license for subsequent Government installation. Submit copies of Auditing Front End Software if this function is not part of the software provided with the control system to meet requirements of other Sections.

3.5.3.1 Import and Upload Requirements

Auditing Front End Software must be capable of importing audit logs from the Device Audit Record Upload Software and of uploading audit logs over the network from all control system devices supporting network upload of audit logs.

3.5.3.2 Export Requirements

Auditing Front End Software must be capable of exporting to a file format supported by Microsoft Excel.

3.5.4 Audit Storage Capacity and Audit Upload

{For Government Reference Only: This subpart (and its subparts) relates to AU-4; CCI-001848, CCI-001849}

The creation of audit records must never interfere with normal device operation. Devices must cease collection of auditing information if required to maintain normal operation.

- a. For devices that have STIG/SRGs related to audit storage capacity (CCI-001848 or CCI-001849) comply with the requirements of those STIG/SRGs.
- b. For controllers capable of generating audit records, provide 60 days worth of secure local storage, assuming 10auditable events per day.

3.5.4.1 [Device Audit Record Upload Software](#)

For each device (computer or controller) required to audit events and for which audit logs cannot be uploaded over the network by the Auditing Front End Software, provide and license to the Government software implementing a secure mechanism of uploading audit records from the device and exporting them to the Auditing Front End Software. Where different devices use different software, provide software of each type required to upload audit logs from all devices.

Submit copies of device audit record upload software if this function is not part of the software provided with the control system to meet requirements of other Sections. If there are no devices requiring this software, provide a document stating this in lieu of this submittal.

3.5.5 Response to Audit Processing Failures

{For Government Reference Only: This subpart (and its subparts) relates to AU-5; CCI-000139, CCI-000140, CCI-001490.}

In the case of a failure in the auditing system, computers associated with auditing must provide email notification. In case of an audit failure, if possible, continue to collect audit records by overwriting existing audit records.

3.6 REQUIREMENTS FOR LEAST FUNCTIONALITY

{For Government Reference Only: This subpart (and its subparts), along with the Network Communication, Ports, Protocols and Services Report submittal specified elsewhere in this section, relates to CM-6(a), CM-6(c), CM-7, CM-7(1)(b), SC-41; CCI-000363, CCI-000364, CCI-000365, CCI-001588, CCI-001755, CCI-000381, CCI-000380, CCI-000382, CCI-001761, CCI-001762, CCI-002544, CCI-002545, CCI-002546. }

For devices that have a STIG or SRG related to Requirements for Least Functionality (such as configuration settings and port and device I/O access for least functionality), install and configure the

device in accordance with that STIG or SRGs.

3.6.1 Device Capabilities

For HVAC Control Systems: Do not provide devices with remote user interfaces or with full user interfaces where one was not required. Do not use a networked sensor or actuator where a non-networked sensor or actuator would suffice.

For Other Control Systems: Do not provide devices with remote user interfaces or with full user interfaces where one was not required.

3.6.2 Software

For software that has a STIG or SRG related to Requirements for Least Functionality (such as configuration settings and port access for least functionality), install and configure the software in accordance with that STIG or SRG.

Do not install software that is not specifically required to meet a contract requirement. Remove any previously installed that is not specifically required to meet a contract requirement. Do not implement functionality within software that is not specifically required to meet contract requirements.

3.7 SYSTEM AND COMMUNICATION PROTECTION

3.7.1 Collaborative Computing

{For Government Reference Only: This subpart relates to SC-15(a), SC-15(b); CCI-001150, CCI-001152.}

Without explicit approval from the project site, control systems must not use collaborative computing technologies.

3.7.2 Denial of Service Protection

{For Government Reference Only: This subpart relates to SC-5, SC-12, SC-7(a); CCI-001093, CCI-002385, CCI-002386, CCI-002430, CCI-001097. }

To the greatest extent practical, implement control logic without reliance on the network. Except when required to meet the requirements of the control system Section (where the requirement can only be met using computer hardware), do not implement control logic in computers.

3.8 SAFE MODE AND FAIL SAFE OPERATION

{For Government Reference Only: This subpart (and its subparts) relates to CP-12, SI-10(3), SI-17; CCI-002855, CCI-002856, CCI-002857, CCI-002754, CCI-002773, CCI-002774, CCI-002775}

For all control system components with an applicable STIG or SRG, configure the component in accordance with all applicable STIGs and SRGs.

3.9 SYSTEM MAINTENANCE TOOL SOFTWARE

{For Government Reference Only: This subpart (and its subparts) relates to MA-3; CCI-000865.}

Submit and license to the Government all software required to operate, maintain and modify the control system such the Government or their agents are able to perform repair, replacement, upgrades, and expansions of the system without subsequent or future dependence on the Contractor, Vendor or Manufacturer. Submit hard copies of user manuals for each software with the software submittal. Provide any hardware keys or dongles, software keys, license numbers, and other

information required to enable the Government to access or change the system.

For software provided and licensed to the Government under the requirements of another Section, submit a statement indicating the Section and Submittal under which the software was provided. For software provided to meet the requirements of this Section and not provided and licensed under another Section, submit software and software user manuals on DVD or CD as a Technical Data Package and submit one hard copy of the software user manual for each piece of software.

3.10 DEVICE POWER

{For Government Reference Only: This subpart (and its subparts) relates to PE-11, PE-11(1); CCI-002955, CCI-000961. }

For LOW Impact Systems: Provide emergency power in accordance with the control system and equipment specification Sections.

3.11 VULNERABILITY SCANNING

{For Government Reference Only: This subpart (and its subparts) relates to RA-5 RA-5(a),RA-5(b),RA-5(c),RA-5(d); CCI-001054, CCI-001055, CCI-000156, CCI-001641, CCI-001643, CCI-001057, CCI-001058, CCI-001059. }

All IP devices must be scannable, such that the device can be scanned by industry standard IP network scanning utilities without harm to the device, application, or functionality.

3.11.1 Computers and Software Running on Computers

Computers and applications running on computers must meet relevant vulnerability scanning STIGs/SRGs and respond to approved DoD vulnerability scanning tools.

3.11.2 Controllers

Provide controllers that are scannable by standard control system discovery tools or control system browsers and return meaningful status information including the network inputs and outputs for the controller. This information must contain sufficient detail to detect vulnerabilities or exploits of the controller.

Provide all software needed to scan the control system as the [Control System Scanning Tools](#) submittal. If the software required to scan the system is already installed at the project site or is provided under a separate section instead provide a statement indicating this.

3.12 FIPS 201-2 REQUIREMENT

{For Government Reference Only: This subpart (and its subparts) relates to SA-4 (10); CCI-003116}

Devices in the following systems which implement PIV must be on the [NIST FIPS 201-2](https://www.idmanagement.gov/approved-products-list/) approved product list (<https://www.idmanagement.gov/approved-products-list/>): NONE.

3.13 SYSTEM AND INTEGRATION INTEGRITY

3.13.1 Malicious Code Protection

{For Government Reference Only: This subpart (and its subparts) relates to SI-3(c); CCI-001241, CCI-002623}

For all computers installed under this project, provide malware protection software media, provide licenses, and install and configure malware protection software as indicated. Coordinate with the Government Computer Access Point of Contact as required.

- a. Provide malware protection software licenses.
- b. Provide malware protection software media.
- c. Install and configure malware protection software in accordance with the relevant STIGs.

3.14 CONTROL SYSTEM CYBERSECURITY TESTING

3.14.1 Control System Cybersecurity Testing Procedures

Prepare and submit Control System Cybersecurity Testing Procedures explaining step-by-step, the actions and expected results that will demonstrate that the control system meets the requirements of this Section. The Control System Cybersecurity Testing Procedures may be submitted as a Technical Data Package.

3.14.2 Control System Cybersecurity Testing Execution

Using the Control System Cybersecurity Testing Procedures verify that the control system meets the requirements of this Section. **UNLESS GOVERNMENT WITNESSING OF A TEST IS SPECIFICALLY WAIVED BY THE GOVERNMENT, PERFORM ALL TESTS WITH A GOVERNMENT WITNESS.** If testing reveals deficiencies in the system, correct the deficiency and retest until successful.

3.14.3 Control System Cybersecurity Testing Report

Prepare and submit a Control System Cybersecurity Testing Report documenting all tests performed and their results. Include all tests in the Control System Cybersecurity Testing Procedures and any additional tests performed during testing. Document test failures and repairs conducted with the test results. The Control System Cybersecurity Testing Report may be submitted as a Technical Data Package

3.15 FIELD QUALITY CONTROL, CYBERSECURITY VALIDATION SUPPORT

AM0003* In addition to testing and testing support required by other Sections, provide a minimum of ~~120~~40 hours of technical support for cybersecurity testing of control systems to support the DoD Risk Management Framework process Cybersecurity assessment of the control system. This support is independent of (and in addition to) the Control System Cybersecurity Testing specified in this section.

***AM0003**

3.16 CYBERSECURITY TRAINING

Provide eight hours of classroom and hands-on training for six Government personnel on the cybersecurity operation and maintenance of the control system provided. This training is in addition to and must be coordinated with control system training specified in other Sections.

The Government will provide the training location. Training must cover, at a minimum: (a) applying software and firmware updates, (b) user account creation, modification and deletion, (c) audit log upload procedures and (d) identification of privileged user interfaces and system impact of those interfaces. Training session must include a question and answer period during which government staff questions about cybersecurity aspects of the control system are answered.

-- End of Section --

SECTION TABLE OF CONTENTS

DIVISION 25 - INTEGRATED AUTOMATION

SECTION 25 05 11.02

CYBERSECURITY FOR FACILITY-RELATED CONTROL SYSTEMS: FIRE ALARM/MASS NOTIFICATION SYSTEM

PART 1 GENERAL

- 1.1 CONTROL SYSTEM APPLICABILITY
- 1.2 RELATED REQUIREMENTS
- 1.3 REFERENCES
- 1.4 DEFINITIONS
 - 1.4.1 Administrator Account
 - 1.4.2 Computer
 - 1.4.3 Controller
 - 1.4.4 Mission Space
 - 1.4.5 Network
 - 1.4.6 Network Connected
 - 1.4.6.1 Wireless Network Connected
 - 1.4.7 Network Media
 - 1.4.8 User Account Support Levels
 - 1.4.8.1 FULLY Supported
 - 1.4.8.2 MINIMALLY Supported
 - 1.4.8.3 NOT Supported
 - 1.4.9 Manual Local Input
 - 1.4.10 Card Reader
 - 1.4.11 User Interface
 - 1.4.11.1 Local User Interface
 - 1.4.11.2 Remote User Interface
 - 1.4.11.3 Types of User Interface (by capability)
 - 1.4.11.3.1 Read-Only User Interface
 - 1.4.11.3.2 Limited User Interface
 - 1.4.11.3.3 Full User Interface
 - 1.4.11.3.4 View-Only User Interface
 - 1.4.11.4 Other User Interface Terminology
 - 1.4.11.4.1 Writable User Interface
 - 1.4.11.4.2 Privileged User Interface
 - 1.4.12 Wireless Network
 - 1.4.13 Wired Broadcast Network
- 1.5 ADMINISTRATIVE REQUIREMENTS
 - 1.5.1 Points of Contact
 - 1.5.2 Coordination
- 1.6 SUBMITTALS
- 1.7 CYBERSECURITY DOCUMENTATION
 - 1.7.1 Proposed STIG and SRG Applicability Report
 - 1.7.2 Cybersecurity Interconnection Schedule
 - 1.7.3 Network Communication, Ports, Protocols and Services Report
 - 1.7.4 Control System Inventory Reports
 - 1.7.5 Software and Configuration Backups
 - 1.7.6 Cybersecurity Network (Riser) Diagram
 - 1.7.7 STIG, SRG and Vendor Guide Compliance Result Report

- 1.7.8 Control System Cybersecurity Documentation
 - 1.7.8.1 Software Applications
 - 1.7.8.2 Default Requirements for Control System Devices
- 1.8 SOFTWARE LICENSING
- 1.9 CYBERSECURITY DURING CONSTRUCTION
 - 1.9.1 Contractor Computer Equipment
 - 1.9.1.1 Operating System
 - 1.9.1.2 Anti-Malware Software
 - 1.9.1.3 Passwords and Passphrases
 - 1.9.1.4 User-Based Authentication
 - 1.9.1.5 Demonstration of Compliance
 - 1.9.1.6 Contractor Computer Cybersecurity Compliance Statements
 - 1.9.2 Temporary IP Networks
 - 1.9.2.1 Network Boundaries and Connections
 - 1.9.3 Government Access to Network
 - 1.9.4 Passwords and Passphrases
 - 1.9.5 Contractor Temporary Network Cybersecurity Compliance Statements
- 1.10 CYBERSECURITY DURING WARRANTY PERIOD

PART 2 PRODUCTS

- 2.1 ETHERNET SWITCH
 - 2.1.1 Required Functionality
 - 2.1.2 Configuration Requirements
- 2.2 DAISY CHAIN IP CONTROLLERS
- 2.3 DATABASE AND WEB SERVER SOFTWARE FOR MODERATE IMPACT SYSTEMS

PART 3 EXECUTION

- 3.1 CYBERSECURITY HARDENING AND CONFIGURATION GUIDES
- 3.2 NETWORK REQUIREMENTS
 - 3.2.1 Information Flow Enforcement In MODERATE Impact Systems
 - 3.2.2 Wireless and Wired Broadcast Communication for Fire Protection Systems
 - 3.2.3 Wireless and Wired Broadcast Communication for Systems Other than Fire Protection Systems
 - 3.2.3.1 Wireless and Wired Broadcast IP Communications
 - 3.2.3.2 Non-IP Wireless Communication
 - 3.2.3.3 Wireless and Wired Broadcast Communication Request
 - 3.2.4 Non-IP Control Networks
 - 3.2.5 IP Control Networks
 - 3.2.5.1 IP Network Routers
 - 3.2.5.2 IP Devices With Multiple Ethernet Connections
 - 3.2.6 Cryptographic Protection
 - 3.2.7 Device Identification and Authentication
 - 3.2.8 Cryptographic Module Authentication
- 3.3 ACCESS CONTROL REQUIREMENTS
 - 3.3.1 User Accounts
 - 3.3.1.1 Computers
 - 3.3.1.2 Controllers
 - 3.3.1.2.1 Fire Protection Systems
 - 3.3.1.3 Additional User Account Expiration Requirements In MODERATE Impact Systems:
 - 3.3.1.3.1 For Control System Applications Running on Computers
 - 3.3.1.3.2 For Other Control System Devices FULLY Supporting Accounts
 - 3.3.2 Unsuccessful Logon Attempts
 - 3.3.2.1 Devices MINIMALLY Supporting Accounts
 - 3.3.2.2 Devices FULLY Supporting Accounts
 - 3.3.2.3 High Availability Interfaces Exempt from Unsuccessful Logon Attempts Requirements
 - 3.3.3 System Use Notification
 - 3.3.3.1 System Use Notification for Remote User Interfaces

- 3.3.3.2 System Use Notification for Local User Interfaces
- 3.3.4 Session Lock and Session Termination Requirements In MODERATE Impact Systems:
 - 3.3.4.1 Session Termination
 - 3.3.4.2 Session Lock
 - 3.3.4.3 Session Lock and Termination for Computers
 - 3.3.4.4 Session Lock and Termination for Controllers
- 3.3.5 Permitted Actions Without Identification or Authentication
- 3.3.6 Physical Security in MODERATE Impact Systems
 - 3.3.6.1 Physical Security for Media
 - 3.3.6.1.1 Physical Security for Media Inside Mission Space
 - 3.3.6.1.2 Physical Security for Media Outside Mission Space
 - 3.3.6.1.3 Physical Security for Non-Network Media in Fire Protection Systems
 - 3.3.6.2 Physical Security for Devices
 - 3.3.6.2.1 Physical Security for Devices in Fire Protection Systems
 - 3.3.6.3 Physical Security for User Interfaces
- 3.3.7 Enclosures
- 3.4 USER IDENTIFICATION AND AUTHENTICATION
 - 3.4.1 User Identification and Authentication for All System Types
 - 3.4.2 User Identification and Authentication for Specific System Types
 - 3.4.3 User Identification and Authentication for Specific Devices
 - 3.4.4 Implementation of Identification and Authorization Requirements
 - 3.4.5 Password-Based Authentication Requirements
 - 3.4.5.1 Passwords for Software and Applications Running on Computers
 - 3.4.5.2 Passwords for Controllers FULLY Supporting Accounts
 - 3.4.5.3 Passwords for Remote Interfaces
 - 3.4.5.4 Passwords for Devices Minimally Supporting Accounts
 - 3.4.5.5 Password Configuration and Reporting
 - 3.4.6 Authenticator Feedback
 - 3.4.7 Implementation of PKI Infrastructure in Moderate Impact Systems
- 3.5 CYBERSECURITY AUDITING
 - 3.5.1 Audit Events, Content of Audit Records, and Audit Generation
 - 3.5.1.1 Computers
 - 3.5.1.1.1 Audited Events
 - 3.5.1.1.2 Audit Event Information To Record
 - 3.5.2 Audit Time Stamps
 - 3.5.3 Auditing Front End Software
 - 3.5.3.1 Import and Upload Requirements
 - 3.5.3.2 Export Requirements
 - 3.5.3.3 Notification Of Audit Failure in Devices in MODERATE Impact Systems
 - 3.5.3.4 Audit Reduction and Report Generation In MODERATE Impact Systems
 - 3.5.4 Audit Storage Capacity and Audit Upload
 - 3.5.4.1 Audit Log Storage Notification In MODERATE Impact Systems
 - 3.5.4.2 Device Audit Record Upload Software
 - 3.5.5 Response to Audit Processing Failures
- 3.6 REQUIREMENTS FOR LEAST FUNCTIONALITY
 - 3.6.1 Device Capabilities
 - 3.6.2 Software
- 3.7 SYSTEM AND COMMUNICATION PROTECTION
 - 3.7.1 Collaborative Computing
 - 3.7.2 Denial of Service Protection and Application Partitioning In MODERATE Impact Systems:
 - 3.7.2.1 Default Requirements for MODERATE Impact Control Systems
 - 3.7.3 Mobile Code In MODERATE Impact Systems:
 - 3.7.4 Protection of Information at Rest In MODERATE Impact Systems:
 - 3.7.5 Process Isolation and Boundary Protection in Moderate Impact Fire Protection Systems
 - 3.7.5.1 Radio Interfaces for Fire Protection Systems
 - 3.7.5.2 Fire Suppression System Network Isolation
- 3.8 SAFE MODE AND FAIL SAFE OPERATION
- 3.9 SYSTEM MAINTENANCE TOOL SOFTWARE
- 3.10 DEVICE POWER

- 3.10.1 Device Behavior on Loss of Power In MODERATE Impact Systems:
- 3.11 VULNERABILITY SCANNING
 - 3.11.1 Computers and Software Running on Computers
 - 3.11.2 Controllers
- 3.12 SYSTEM AND INTEGRATION INTEGRITY
 - 3.12.1 Malicious Code Protection
 - 3.12.2 Software, Firmware, and Information Integrity In MODERATE Impact Systems:
- 3.13 CONTROL SYSTEM CYBERSECURITY TESTING
 - 3.13.1 Control System Cybersecurity Testing Procedures
 - 3.13.2 Control System Cybersecurity Testing Execution
 - 3.13.3 Control System Cybersecurity Testing Report
- 3.14 FIELD QUALITY CONTROL, CYBERSECURITY VALIDATION SUPPORT
- 3.15 CYBERSECURITY TRAINING

AM0003*

*AM0003

-- End of Section Table of Contents --

SECTION 25 05 11.02

CYBERSECURITY FOR FACILITY-RELATED CONTROL SYSTEMS: FIRE ALARM/MASS NOTIFICATION SYSTEM

PART 1 GENERAL

Many subparts in this Section contain text in curly braces ("{" and "}") indicating which cybersecurity control and control correlation identifier (CCI) the requirements of the subpart relate to. The text inside these curly braces is for Government reference only and enables coordination of the requirements of this Section with the RMF process throughout the design and construction process. Text in curly braces are not contractor requirements.

This Section refers to Security Requirements Guide (SRGs) and Security Technical Implementation Guide (STIGs). STIGs and SRGs are available online at the Information Assurance Support Environment (IASE) website at <https://public.cyber.mil/stigs/downloads/> and an SRG/STIG Applicability Guide and Collection Tool is available at <https://public.cyber.mil/stigs/SCAP/>. Not all control system components have applicable STIGs or SRGs. The "Control Systems SRG" does not apply to work performed under this Section; all requirements within this section to apply applicable SRGs DO NOT include the "Control Systems SRG".

1.1 CONTROL SYSTEM APPLICABILITY

There are multiple versions of this Section associated with this project. Different versions have requirements applicable to different control systems. This specific Section applies only to the following control systems: Fire Alarm/Mass Notification System.

1.2 RELATED REQUIREMENTS

This section does not contain sufficient requirements to procure a control system and must be used in conjunction with other Sections which specify control systems. This Section adds cybersecurity requirements to the control systems specified in other Sections, and as these requirements are conditioned on the control system being provided, there may be requirements in this Section that will not apply to this project. All Sections containing facility-related control systems or control system components are related to the requirements of this Section. Review all specification sections to determine related requirements.

In cases where a requirement is specified in both this Section and in another Section, the more stringent requirement must be met. In cases where a requirement in this Section conflicts with the requirements of another Section such that both requirements cannot be met at the same time, request direction from the Contracting Officer to determine which requirement applies to the project.

1.3 REFERENCES

The publications listed below form a part of this specification to the extent referenced. The publications are referred to within the text by the basic designation only.

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS (IEEE)

IEEE 802.1x

(2010) Local and Metropolitan Area Networks - Port Based
Network Access Control

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

NIST FIPS 140-2

(2001) Security Requirements for Cryptographic Modules

U.S. DEPARTMENT OF DEFENSE (DOD)

DODI 8551.01

(2014) Ports, Protocols, and Services Management
(PPSM)

DTM 08-060

(2008) Policy on Use of Department of Defense (DoD)
Information Systems - Standard Consent Banner and User
Agreement

1.4 DEFINITIONS

1.4.1 Administrator Account

An administrator account is an account with full permissions to a device, application, or operating system, including the ability to create and modify other user accounts.

Note that the operating system Administrator Account may be different than Administrator Accounts for applications hosted on that operating system. Also, most controllers will not have any support for accounts and will therefore not have an 'Administrator Account'.

1.4.2 Computer

A computer is one of the following:

- a. a device running a non-embedded desktop or server version of Microsoft Windows
- b. a device running a non-embedded version of MacOS
- c. a device running a non-embedded version of Linux
- d. a device running a version or derivative of the Android Operating System, where Android is considered separate from Linux
- e. a device running a version of Apple iOS

Unless otherwise indicated or clear from context use of the word "device" in this Section includes computers.

1.4.3 Controller

A device other than a computer or Ethernet switch. [For Fire Protection systems this includes fire alarm control panels, remote operating consoles, and remote annunciators.](#)

1.4.4 Mission Space

A device or media is in mission space if physical access to the device or media is controlled by the organization served by the device. For example, a variable air volume (VAV) box controller in a suspended ceiling is in mission space if the VAV box serves that room; an electrical switchgear in an electrical room or an air handling unit (AHU) in a mechanical room or on a rooftop may still be considered to be in mission space if the organization (mission) served by that switchgear or AHU controls access to the electrical room, mechanical room or rooftop.

1.4.5 Network

A network is a group of two or more devices that can communicate using a network protocol. Network protocols must provide a method for addressing devices on the network; a communication method that does not provide an addressing scheme is not a networked form of communication. Devices that communicate using a method of communication that does not support device addressing are not using a network. Addresses may be other than IP addresses, and addressing may be at either Open

Systems Interconnection (OSI) layer 2 or layer 3.

1.4.6 Network Connected

A component is network connected (or "connected to a network") only when the device has a network transceiver which is directly connected to the network and implements the network protocol. A device lacking a network transceiver (and accompanying protocol implementation) can never be considered network connected. Note that (unlike many IT definitions of "Network Connected") a device connected to a non-IP network is still considered network connected (an IP connection or IP address is not required for a device to be network connected).

1.4.6.1 Wireless Network Connected

Any device that supports wireless network communication is network connected to a wireless network, regardless of whether the device is communicating using wireless. Unless physically disabled, devices with wireless transceivers support wireless, it is not sufficient to disable the wireless in software.

1.4.7 Network Media

The thing that provides the communication channel between the devices on a network. Typically wire, but might include wireless, fiber optic, or even power line (some network protocols allow sending network signals over power wiring).

1.4.8 User Account Support Levels

The support for user accounts is categorized in this Section as one of three levels:

1.4.8.1 FULLY Supported

Device supports configurable individual accounts. Accounts can be created, deleted, modified, etc. Privileges can be assigned to accounts. These devices support user-based (as opposed to role-based) authentication.

1.4.8.2 MINIMALLY Supported

Device supports a small, fixed number of accounts (perhaps only one). Accounts cannot be modified. A device with only a "User" and an "Administrator" account would fit this category. Similarly, a device with two PINs for logon - one for restricted and one for unrestricted rights would fit here (in other words, the accounts do not have to be the traditional "username and password" structure). These devices typically only support role-based authentication.

Examples of devices which MINIMALLY support accounts are a) a variable frequency drive with a single account which requires a PIN for access to configuration; and b) a room lighting control touchpad interface that has a single account.

1.4.8.3 NOT Supported

Device does not support any Access Enforcement therefore the whole concept of "account" is meaningless.

1.4.9 Manual Local Input

Manual Local Inputs are system analog or binary inputs that are adjustable by a person but are, by intrinsic hardware design, very limited in potential capabilities. Manual Local Inputs do not have touch screens or full keyboards, but may have a few buttons or dials to allow input. Manual Local Inputs do not have full graphic screens or dot-matrix displays, but may have simple lights (LEDs) or 7-segment displays. Manual Local Inputs do not have any sort of menu structure, each button has a single well-defined function.

Examples of Manual Local Inputs are H-O-A switches, simple thermostats, and disconnect switches.

1.4.10 Card Reader

A card reader is an input/output device whose primary function is to assist in two-factor authentication. A card reader must have an interface to read data from a card and may be able to write data to a card. A card reader may have a means (such as buttons, keypad, touchscreen, etc.) for a user to input a PIN or password, as well as a limited display.

1.4.11 User Interface

A User Interface (UI) is something other than a Manual Local Input or Card Reader that allows a person to interact with the system or device. Note that while a Card Reader is not by itself a User Interface, a User Interface may contain a Card Reader in order for it to authenticate its user. Within control systems, there are a wide range of User Interfaces.

Two important distinctions are 1) whether the user interface is Local or Remote, and 2) the effective capabilities of the User Interface to alter data, which is the "privilege" of the user interface (where effective privilege available to a specific user at a specific user interface is the combination of the greatest privilege offered by the user interface and the specific account the user is logged into).

1.4.11.1 Local User Interface

A Local User Interface is a user interface where the physical hardware the user interacts with (keyboard, buttons, display, etc.) is physically part of the device being affected. All of the relevant characteristics of the user interface are embodied within a single device.

Note that a Local UI may be able to access data in a different device, Local versus Remote in this context refers to the user interface itself; the capability to access data in a different device is covered under "Full User Interface".

1.4.11.2 Remote User Interface

A Remote User Interface implements a Client/Server model where the physical hardware the user interacts with (Client) is physically distinct from the device being affected (Server). Most or all of the security and functionality characteristics of the user interface are defined by the Server, not the Client. The Client and Server communicate via a network connection. A common example of a remote user interface is a web-based interface where the browser (client) is generally on different hardware than the web server (server). A Remote UI remains a Remote UI even if the user happens to be at a Client on the same hardware as the Server. What is important is that a) the Client may be on different hardware than the Server and b) the majority of the security and functional characteristics of the interface are defined at the Server.

Note that this definition of "remote" is consistent with that generally used in the control industry but is not aligned with the NIST 800-53 definition of "Remote", which refers to "outside the system". The term "Remote" here better aligns with the NIST 800-53 definition of "Network" (remote from within the system) Access.

1.4.11.3 Types of User Interface (by capability)

User interfaces are also categorized by their capabilities as being Read Only, Limited, or Full.

1.4.11.3.1 Read-Only User Interface

A Read Only User Interface (also referred to as a View-Only User Interface) is a user interface that only allows for reading data, it does not allow (have the capability to) modify data. A Read Only User Interface may be either Local or Remote. A User Interface that is configured to be Read Only (by some other means than the interface itself, such as using configuration software on a laptop) is a Read-Only Interface. Note a Read Only User Interface may have buttons (or touch screen, etc.)

allowing the user to navigate through the presentation of data.

Examples of a Read Only User Interfaces are a) a publicly viewable "energy dashboard" showing weather data and energy usage within a building and b) digital wayfinding signage.

1.4.11.3.2 Limited User Interface

A Limited User Interface is a user interface that - by design - can only alter information local to the user interface. Note that the determination of "alter" includes only direct interactions, it explicitly excludes interactions that might occur as secondary effects. For example, an interface changing the flow setpoint in a pump controller is a direct interaction, the subsequent change in flow (as well as any subsequent downstream changes in valve position) are not direct interactions.

Two examples of LIMITED UIs are: a) a variable speed drive has a Limited Local User Interface which allows the user to change properties within the drive, but does not allow affecting things outside the drive; and b) a typical home WiFi Router has a Limited Remote User Interface which allows configuration of the Router, but does not allow direct interaction with other devices.

1.4.11.3.3 Full User Interface

A Full User Interface can alter information in devices outside the device with the user interface. For example, a typical Local Display Panel is a Full Local User Interface while a browser-based front end is a Full Remote User Interface.

1.4.11.3.4 View-Only User Interface

See Read-Only User Interface

1.4.11.4 Other User Interface Terminology

In addition to defining whether a user interface is a Hardware Limited, Read-Only, Limited or Full, and whether it is Local or Remote, user interfaces are classified by whether they are writable or privileged.

1.4.11.4.1 Writable User Interface

Any User Interface that is not Read-Only is Writable. (Limited User Interfaces and Full User Interfaces are both writable user interfaces (as they are capable of changing a value)).

1.4.11.4.2 Privileged User Interface

A Privileged UI is a UI that has sufficient capabilities or functionality that it requires specific cybersecurity measures to be put in place to limit its unauthorized use. Ultimately, whether a specific user interface is considered a Privileged User Interface must be determined by usage. Unless otherwise specified, user interfaces can be determined to be privileged or not using the following:

- a. Read-Only User Interfaces are not privileged user interfaces.
- b. User Interfaces that can inhibit or force the activation of a fire suppression system (e.g. such as for a pre-action or deluge system) are always privileged user interfaces. Other Full User interfaces for Fire Alarm Systems are privileged user interfaces as indicated and shown, or when another requirement of this Section establishes they are privileged. For all other systems, Full User Interfaces are privileged user interfaces.
- c. User interfaces that allow for configuration of auditing or allows for modification or deletion of audit logs are privileged user interface.
- d. User interfaces that allow for reprogramming a network connected device is a privileged user interface.

- e. Except as specified above, a Limited User Interface must be determined to be privileged or not based on the specific capabilities and use case of the user interface. In general however, user interfaces that do not offer significant capabilities above and beyond those available at that location via other means (e.g. such as a disconnect switch, breaker, or hand-off-auto switch, or physical attack) are not privileged.

1.4.12 Wireless Network

Any network that communicates without using wires or fiber optics as the communication media. Wireless networks include: WiFi, Bluetooth, ZigBee, cellular, satellite, long and short wave radio, 2.4 GHz, free space optical, point-to-point laser, microwave, and IR.

1.4.13 Wired Broadcast Network

Wired Broadcast Networks are any network, such as powerline carrier networks and modem (wired telephony), that use wire-based technologies where there is not a clearly defined boundary for signal propagation.

1.5 ADMINISTRATIVE REQUIREMENTS

1.5.1 Points of Contact

Coordinate with the following Points of Contact as indicated in this Section and as required. Not all projects will require coordination with all Points of Contact. When coordination is required and no Point of Contact is indicated, coordinate with the Contracting Officer (KO).

- a. Government Computer Access Point of Contact: Contracting Office (KO)
- b. HTTPS Certificate Point of Contact: Contracting Officer (KO)
- c. Email Address Point of Contact: Contracting Officer (KO)
- d. Password Point of Contact: Contracting Officer (KO)
- e. Mobile Code Point of Contact: Contracting Officer (KO)
- f. PKI Infrastructure Point of Contact: Contracting Officer (KO)

1.5.2 Coordination

Coordinate the execution of this Section with the execution of all other Sections related to control systems as indicated in the paragraph RELATED REQUIREMENTS. Items that must be considered when coordinating project efforts include but are not limited to:

- a. If requesting permission for wireless or wired broadcast communication, the Wireless and Wired Broadcast Communication Request submittal must be approved prior to control system device selection and installation.
- b. If requesting permission for alternate account lock permissions, the Device Account Lock Exception Request must be approved prior to control system device selection and installation.
- c. If requesting permission for the use of a device with multiple physical connections to IP networks, the Multiple IP Connection Device Request must be approved prior to control system device selection and installation.
- d. Wireless testing may be required as part of the control system testing. See requirements for the Wireless Communication Test Report submittal.
- e. If the Device Audit Record Upload Software is to be installed on a computer not being provided as

part of the control system, coordination is required to identify the computer on which to install the software.

- f. The Cybersecurity Interconnection Schedule must be coordinated with other work that will be interconnected to, and interconnections must be approved by the Government before relying on them for system functionality.
- g. Cybersecurity testing support must be coordinated across control systems and with the Government cybersecurity testing schedule.
- h. Passwords must be coordinated with the indicated contact for the project site.
- i. If applicable, HTTPS web server certificates must be obtained from the indicated HTTPS Certificate Point of Contact.
- j. Contractor Computer Cybersecurity Compliance Statements must be provided for each contractor using contractor owned computers.

1.6 SUBMITTALS

Government approval is required for submittals with a "G" or "S" classification. Submittals not having a "G" or "S" classification are for information only. When used, a code following the "G" classification identifies the office that will review the submittal for the Government. Submit the following in accordance with Section 01 33 00 SUBMITTAL PROCEDURES:

SD-01 Preconstruction Submittals

Wireless and Wired Broadcast Communication Request; G

Device Account Lock Exception Request; G

Multiple Ethernet Connection Device Request; G

Contractor Computer Cybersecurity Compliance Statements; G

Contractor Temporary Network Cybersecurity Compliance Statements; G

Cybersecurity Interconnection Schedule ; G

Protection of Information At Rest Proposal; G

Proposed STIG and SRG Applicability Report; G

Pre-Construction Control System Inventory Report ; G

SD-02 Shop Drawings

Network Communication, Ports, Protocols and Services Report; G

Cybersecurity Network (Riser) Diagram ; G

SD-03 Product Data

Control System Cybersecurity Documentation; G

SD-06 Test Reports

Control System Cybersecurity Testing Procedures; G

Control System Cybersecurity Testing Report; G

SD-07 Certificates

Software Licenses; G

SD-11 Closeout Submittals

Confidential Password Report; G

Enclosure Keys; G

Software and Configuration Backups; G

Auditing Front End Software; G

Device Audit Record Upload Software; G

System Maintenance Tool Software; G

Control System Scanning Tools; G

STIG, SRG and Vendor Guide Compliance Result Report; G

Final Control System Inventory Report; G

Integrity Verification Software; G

1.7 CYBERSECURITY DOCUMENTATION

{For Government Reference Only: This subpart (and its subparts) relates to PL-7; CCI-003071}

1.7.1 Proposed STIG and SRG Applicability Report

For each model of network connected or network infrastructure device, use the DISA SRG/STIG Applicability Guide and Collection Tool (available at <https://public.cyber.mil/stigs/SCAP/>) to identify applicable STIGs or SRGs and provide a report indicating applicable STIGs and SRGs for each model. Provide the Proposed STIG and SRG Applicability Report concurrently with the Pre-Construction Control System Inventory Report.

1.7.2 Cybersecurity Interconnection Schedule

{For Government Reference Only: This subpart relates to CA-3(b), PL-8, SC-7(9), SC-7(11); CCI-000258, CCI-003072, CCI-003073, CCI-003075, CCI-002398, CCI-002399, CCI-002401, CCI-002402, CCI-002403. For MODERATE Impact systems, this subpart also relates to SC-7; CCI-001126, CCI-001109}

Provide a completed Cybersecurity Interconnection Schedule documenting network connections between the installed system and other systems. Provide the following information for each device directly communicating between systems: Device Identifier, Device Manufacturer, Device Description, Transport layer Protocol, Network Address, Port (if applicable), MAC (Layer 2) address (if applicable), Media, Application Protocol, Service (if applicable), Descriptive Purpose of communication. For communication with other authorized systems also provide the Foreign Destination and POC for Destination. For MODERATE Impact Systems: Also describe the impact of loss of the connection on the control system. If other control system Sections used on this project include submittals documenting this information, provide copies of those submittals to meet this requirement.

In addition to the requirements of Section 01 33 00 SUBMITTAL PROCEDURES, provide the Cybersecurity Interconnection Schedule as an editable Microsoft Excel file (a template Cybersecurity

Interconnection Schedule in Excel format is available at <https://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-25-05-11>.)

1.7.3 Network Communication, Ports, Protocols and Services Report

{For Government Reference Only: This subpart (and its subparts) relates to CA-9, PL-8; CCI-002102, CCI-002103, CCI-002104, CCI-002105, CCI-003072, CCI-003073, CCI-003075 and also the submittal requirements associated with CM-6, CM-7, including CM-7(3), CCI-000388.}

Provide a Network Communication, Ports, Protocols and Services Report. For each networked device, document device identifier and the communication characteristics of the device including communication protocols, services used, encryption employed, and a general description of what information is communicated over the network. For each device using IP communication, document all TCP and UDP ports used. For each device using non-IP communication, document communication protocol and media used. If other control system Sections used on this project include submittals documenting this information, provide copies of those submittals to meet this requirement.

In addition to the requirements of Section 01 33 00 SUBMITTAL PROCEDURES, provide the Network Communication, Ports, Protocols and Services Report as an editable Microsoft Excel file.

1.7.4 Control System Inventory Reports

{For Government Reference Only: This subpart (and its subparts) relates to CM-8(a), SI-17, IA-3; CCI-000389, CCI-000392, CCI-000398, CCI-002773, CCI-002774, CCI-002775, CCI-000777, CCI-000778, CCI-001958}

Provide a [Pre-Construction Control System Inventory Report](#) report and a [Final Control System Inventory Report](#), using the Inventory Spreadsheet listed under this Section at <https://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-25-05-11>. In the Control System Inventory Reports, document all devices, including networked devices, network infrastructure devices, non-networked devices, input devices (e.g. sensors) and output devices (e.g. actuators). For each device provide all applicable information for which there is a field on the spreadsheet in accordance with the instructions on the spreadsheet.

In addition to the requirements of Section 01 33 00 SUBMITTAL PROCEDURES, provide the Control System Inventory Reports as editable Microsoft Excel files. Provide the Pre-Construction Control System Inventory Report concurrently with the Proposed STIG and SRG Applicability Report

1.7.5 Software and Configuration Backups

{For Government Reference Only: This subpart (and its subparts) relates to CP-10; CCI-000550, CCI-000551, CCI-000552}

For each computer on which software is installed under this project, provide a recovery image of the final as-built computer. This image must allow for bare-metal restore such that restoration of the image is sufficient to restore system operation to the imaged state without the need for re-installation of software. If additional user permissions are required to meet this requirement, coordinate the creation of the image with the identified Government Computer Access Point of Contact.

For all Ethernet switches provide a backup of the switch configuration. For all controllers, provide a backup of the controller configuration and the source code for all loaded application programs (all software that is not common to every controller of the same manufacturer and model).

If any or all of these are provided under another Section, provide documentation indicating this and referencing those submittals.

1.7.6 Cybersecurity Network (Riser) Diagram

{For Government Reference Only: This subpart (and its subparts) relates to PL-2(a), PL-8; CCI-003051, CCI-003053, CCI-003072, CCI-003073, CCI-003075}

Provide a cybersecurity network (riser) diagram of the complete control system including all network and device hardware. For each device, include the device identifier, device type, and manufacturer. If the control system specifications require a riser diagram submittal, provide a copy of that submittal as the cybersecurity riser diagram. Otherwise, provide a riser diagram in one-line format.

1.7.7 STIG, SRG and Vendor Guide Compliance Result Report

For every component (device or software) with an applicable STIG or SRG in the Proposed STIG and SRG Applicability Report, document compliance with the STIG or SRG requirements.

- a. For components which are scannable by the Evaluate-STIG tool (available online at [CAC Required](#)), include the Evaluate-STIG report and raw scan results in addition to the final, manually reviewed and revised, documentation of compliance with STIG and SRG requirements. Checklist files should not contain any findings with a Not Reviewed (NR) status after manual reviews.
- b. For components which do not support automated scanning, a manual review using the General Purpose STIG option should be done. A completed Checklist file should not contain any findings with a Not Reviewed (NR) status after manual reviews

For every component (device or software) with manufacturer provided cybersecurity documentation, procedure, or method for secure configuration or installation, provide a report documenting how the component was configured and any deviation from the manufacturer instructions.

1.7.8 Control System Cybersecurity Documentation

{For Government Reference Only: This subpart (and its subparts) relates to SA-5(a),SA-5(b),SA-5(c), SA-22(b); CCIs: CCI-003124, CCI-003125, CCI-003126, CCI-003127, CCI-003128, CCI-003129, CCI-003130, CCI-003131, CCI-003374}

Provide a Control System Cybersecurity Documentation submittal containing the indicated information for each device and software application.

1.7.8.1 Software Applications

For all software applications running on computers provide:

- a. administrator documentation that describes secure configuration of the software {For Government Reference Only: relates to CCI-003124}
- b. administrator documentation that describes secure installation of the software and software updates. {For Government Reference Only: relates to CCI-003125}
- c. administrator documentation that describes secure operation of the software {For Government Reference Only: relates to CCI-003124}
- d. administrator documentation that describes effective use and maintenance of security functions or mechanisms for the software {For Government Reference Only: relates to CCI-003127}
- e. administrator documentation that describes known vulnerabilities regarding configuration and use of administrative (i.e. privileged) functions for the software {For Government Reference Only: relates to CCI-003128}
- f. user documentation that describes user-accessible security functions or mechanisms in the

software and how to effectively use those security functions or mechanisms {For Government Reference Only: relates to CCI-003129}

- g. user documentation that describes methods for user interaction which enables individuals to use the software in a more secure manner {For Government Reference Only: relates to CCI-003130}
- h. user documentation that describes user responsibilities in maintaining the security of the software {For Government Reference Only: relates to CCI-003131}

1.7.8.2 Default Requirements for Control System Devices

For control system devices where Control System Cybersecurity Documentation requirements are not otherwise indicated in this Section, provide:

- a. Documentation that describes secure configuration of the device {For Government Reference Only: relates to CCI-003124}
- b. Documentation that describes secure installation of the device {For Government Reference Only: relates to CCI-003125}
- c. Documentation that describes secure operation of the device {For Government Reference Only: relates to CCI-003124}
- d. Documentation that describes effective use and maintenance of security functions or mechanisms for the device {For Government Reference Only: relates to CCI-003127}
- e. Documentation that describes known vulnerabilities regarding configuration and use of administrative (i.e. privileged) functions for the device {For Government Reference Only: relates to CCI-003128}
- f. Documentation that describes user-accessible security functions or mechanisms in the device and how to effectively use those security functions or mechanisms {For Government Reference Only: relates to CCI-003129}
- g. Documentation that describes methods for user interaction which enables individuals to use the device in a more secure manner {For Government Reference Only: relates to CCI-003130}
- h. Documentation that describes user responsibilities in maintaining the security of the device {For Government Reference Only: relates to CCI-003131}
- i. Documentation of the published last date of support by the manufacturer or indication that a published date is not available. {For Government Reference Only: relates to CCI-003374}

1.8 SOFTWARE LICENSING

{For Government Reference Only: This subpart (and its subparts) relates to SI-2(a), SI-2(c), SI-7(14); CCI-001227, CCI-002605, CCI-002737}

For all software provided that has not already been licensed to the government or project site, provide a license to the project site for a period of no less than 5 years, and the license must also include the following software updates:

- a. Security and bug-fix patches issued by the software manufacturer.
- b. Security patches to address any vulnerability identified in the National Vulnerability Database at <http://nvd.nist.gov> with a Common Vulnerability Scoring System (CVSS) severity rating of MEDIUM or higher.

Provide a single [Software Licenses](#) submittal with documentation of the software licenses for all

software provided

1.9 CYBERSECURITY DURING CONSTRUCTION

{For Government Reference Only: This subpart (and its subparts) relates to AC-18, CA-3; CCI-000258}

In addition to the control system cybersecurity requirements indicated in this section, meet following requirement throughout the construction process.

1.9.1 Contractor Computer Equipment

Contractor owned computers may be used for construction. Contractor computers connected to the control system, control system network, or a control system component at any point during construction must meet the following requirements:

1.9.1.1 Operating System

The operating system must be an operating system currently supported by the manufacturer of the operating system. The operating system must be current on security patches and operating system manufacturer required updates.

1.9.1.2 Anti-Malware Software

The computer must run anti-malware software from a reputable software manufacturer. Anti-malware software must be a version currently supported by the software manufacturer, must be current on all patches and updates, and must use the latest definitions file. Computers used on this project must perform a full antivirus scan at least once per day. Computers which have connected to any other network since the last full antivirus scan must perform a full antivirus scan prior to connection to the control system network or to the temporary contractor-installed IP network. Perform an antivirus scan on all removable media (e.g., external hard drives, CDs, DVDs, USB flash drives) prior to connecting to the control system environment.

1.9.1.3 Passwords and Passphrases

The passwords and passphrases for computers, applications, and web-based applications supporting passwords must be changed from their default values. Passwords must be a minimum of eight characters with a minimum of one uppercase letter, one lowercase letter, one number and one special character.

1.9.1.4 User-Based Authentication

Each user must have a unique account; sharing of a single account between multiple users is prohibited.

1.9.1.5 Demonstration of Compliance

The Government has the right to require demonstration of computer compliance with these requirements at any time during the project.

1.9.1.6 Contractor Computer Cybersecurity Compliance Statements

Provide a single submittal containing completed Contractor Computer Cybersecurity Compliance Statements for each company using contractor owned computers. Contractor Computer Cybersecurity Compliance Statements must use the template published at <https://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-25-05-11>. Each Statement must be signed by a cybersecurity representative for the relevant company.

1.9.2 Temporary IP Networks

Temporary contractor-installed IP networks may be used during construction. When used, temporary contractor-installed IP networks connected to the control system, control system network, or a control system component at any point during construction must meet the following requirements:

1.9.2.1 Network Boundaries and Connections

The network must not extend outside the project site and must not connect to any IP network other than those specifically provided or furnished for this project. Any and all access to the network from outside the project site is prohibited.

1.9.3 Government Access to Network

Government personnel must be allowed to have complete and immediate access to the network at any time in order to verify compliance with this specification.

1.9.4 Passwords and Passphrases

The passwords and passphrases for all network devices and network access must be changed from their default values. Passwords must be a minimum 8 characters with a minimum of one uppercase letter, one lowercase letter, one number and one special character.

1.9.5 Contractor Temporary Network Cybersecurity Compliance Statements

Provide a single submittal containing completed Contractor Temporary Network Cybersecurity Compliance Statements for each company implementing a temporary IP network. Contractor Temporary Network Cybersecurity Compliance Statements must use the template published at <https://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-25-05-11>. Each Statement must be signed by a cybersecurity representative for the relevant company. If no temporary IP networks will be used, provide a single copy of the Statement indicating this.

1.10 CYBERSECURITY DURING WARRANTY PERIOD

All work performed on the control system after acceptance must be performed using Government Furnished Equipment or equipment specifically and individually approved by the Government.

PART 2 PRODUCTS

All products used on this project must meet the indicated requirements, but not all products specified here will be required by every project.

2.1 ETHERNET SWITCH

Provide Open Systems Interconnection (OSI) Layer 2 Ethernet switches with the following capabilities, and with an interface to support switch configuration for these capabilities:

2.1.1 Required Functionality

Switches must:

- a. Copper Ethernet ports must auto negotiate for 10, 100 and 1000 megabits-per-second links.
- b. Be capable of implementing port level access control by MAC address and limit the number of MAC addresses to one MAC address per port.
- c. For MODERATE Impact Systems, be capable of implementing per-port access control lists (ACLs) where the list can be filtered by source and destination IP addresses, and by source and destination UDP or TCP ports.

2.1.2 Configuration Requirements

Switches must:

- a. Support configuration save and restore.
- b. Support both manual IP address assignment and acquisition of a dynamic IP address via Dynamic Host Configuration Protocol (DHCP).
- c. Be capable of limiting access for configuration to one or more of: a web interface using HTTPS, a command line interface using SSH, or an SNMP connection using SNMP version 3 or later.
- d. Support the ability to lock configuration capability to a dedicated management port.

2.2 DAISY CHAIN IP CONTROLLERS

Controllers used as Daisy Chain IP Controllers must be IP controllers with exactly two Ethernet network connections and basic built-in switch capabilities to allow implementation of an Ethernet network in a daisy chain architecture. Switches incorporated by Daisy Chain IP Controllers are not required to meet the requirements for Ethernet Switches as defined in this Section.

2.3 DATABASE AND WEB SERVER SOFTWARE FOR MODERATE IMPACT SYSTEMS

{For Government Reference Only: This subpart (and its subparts) relate to RA-5(1), RA-5(5); CCI-001062, CCI-001067, CCI-001645, CCI-002906}

All computer-based databases must use Microsoft SQL Server. All computer-based web interfaces must use Internet Information Services (IIS) as the web server.

PART 3 EXECUTION

3.1 CYBERSECURITY HARDENING AND CONFIGURATION GUIDES

Install, configure, and harden all hardware and software furnished on this project in accordance with manufacturer provided documentation, procedures, or methods for secure configuration or installation. Do not implement specific hardening actions if that action would conflict with required functionality or another requirement of this Section.

3.2 NETWORK REQUIREMENTS

3.2.1 Information Flow Enforcement In MODERATE Impact Systems

{For Government Reference Only: This subpart (and its subparts) relate to AC-4; CCI-001368, CCI-001414, CCI-001548, CCI-001549, CCI-001550, CCI-001551}

Install and configure Ethernet switches to block all traffic on all ports not required by the control protocol.

3.2.2 Wireless and Wired Broadcast Communication for Fire Protection Systems

The use of wireless and wired broadcast communication for fire protection systems within a facility is prohibited. Wireless communication may be used to provide communication from the fire protection system in a facility to the central monitoring station. Communication between the fire protection system and the central monitoring station must be via FIPS 140-2 certified devices.

3.2.3 Wireless and Wired Broadcast Communication for Systems Other than Fire Protection Systems

{For Government Reference Only: This subpart (and its subparts) relates to AC-18, AC-18(3);

CCI-001438, CCI-001439, CCI-002323, CCI-001441, CCI-001449}

Unless explicitly authorized by the Government, do not use any wireless or wired broadcast communication.

3.2.3.1 Wireless and Wired Broadcast IP Communications

Do not install wireless or wired broadcast IP networks, including: do not install a wireless access point; do not install or configure an ad-hoc wireless network; do not install or configure a WiFi Direct communication.

When explicitly authorized by the Government, wireless IP communication may be used to communicate with an existing wireless network.

3.2.3.2 Non-IP Wireless Communication

For MODERATE Impact Systems: When non-IP wireless communication is explicitly authorized by the Government, the radios must meet NIST FIPS 140-2 Level 2.

3.2.3.3 Wireless and Wired Broadcast Communication Request

Provide a report documenting the proposed use of wireless or wired broadcast communication prior to device selection using the Wireless and Wired Broadcast Communication Request Schedule at <https://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-25-05-11>. If there is no proposed use of wireless or wired broadcast communication, provide a document indicating this instead of the Request Schedule.

For each device proposed to use wireless or wired broadcast communication show: the device identifier, a description of the device, the location of the device, the device identifiers of other devices communicating with the device, the protocol used for communication, encryption type and strength. For wireless communication, also show: RF Frequency, Radiated Power in dBm (decibel with a milliwatt reference), free-space range, and the expected as-installed range.

3.2.4 Non-IP Control Networks

When control system specifications require particular communication protocols, use only those communication protocols and only as specified. Do not implement any other communication protocol.

When control system specifications do not indicate requirements for communication protocols, use only those protocols required for operation of the system as specified.

3.2.5 IP Control Networks

{For Government Reference Only: This subpart relates to CM-6(a), CM-7(a), CM-7(b), CM-7(1)(b), SC-41; CCI-001588, CCI-000381, CCI-000380, CCI-000381, CCI-000382, CCI-001761, CCI-001762, CCI-002544, CCI-002545, CCI-002546. For Moderate Impact Systems, this subpart (and its subparts) also relates to SC-5(1), SC-5(2); CCI-001094 CCI-001095}

IP Networks must be Ethernet networks and must use switches which are Ethernet Switches or Daisy Chain IP Controllers as defined in this Section. Do not use nonsecure functions, ports, protocols and services as defined in DODI 8551.01 unless those ports, protocols and services are specifically required by the control system specifications or otherwise specifically authorized by the Government. Do not use ports, protocols and services that are not specified in the control system specifications or required for operation of the control system.

For MODERATE Impact Systems, unless explicitly authorized, do not use IP networks if the same control functionality is available through the use of non-IP networks.

3.2.5.1 IP Network Routers

Do not install any device that performs IP routing.

3.2.5.2 IP Devices With Multiple Ethernet Connections

Except for Ethernet Switches and Daisy Chain IP Controllers, devices must not have more than one Ethernet connection to IP networks unless doing so is required by the project specifications and the specific application is approved. If a device with Multiple Ethernet Connections to IP networks is required, provide a [Multiple Ethernet Connection Device Request](#) using the Multiple Ethernet Connection Device Request Template at <https://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-25-05-11> to request approval for each device. If a device with Multiple Ethernet Connections to IP networks is not required, instead provide a document stating that no approval is being requested.

3.2.6 Cryptographic Protection

{For Government Reference Only: This subpart relates to IA-2(9), IA-3(1), SC-8, SC-13, SC-23(1), SC-23(3); CCI-001942, CCI-001959, CCI-001967, CCI-002418, CCI-002449, CCI-002450, CCI-001185, CCI-001188, CCI-001664.}

All remote user interfaces must use HTTPS for all traffic between the user interface client and user interface server.

For devices that have STIG/SRGs related to cryptographic protection (CCI-002450), comply with the requirements of those STIG/SRGs. Ensure that all network traffic is encrypted using NSA-approved cryptography; provision of digital signatures and hashing, and FIPS-validated cryptography.

3.2.7 Device Identification and Authentication

{For Government Reference Only: This subpart (and its subparts) relates to IA-3; CCI-000777, CCI-000778, CCI-001958. [For MODERATE Impact systems, this subpart \(and its subparts\) also relates to SC-23, SC-23\(5\); CCI-001184, CCI-002470.](#)}

All computers must support and implement [IEEE 802.1x](#) for device authentication to the network.

3.2.8 Cryptographic Module Authentication

{For Government Reference Only: This subpart (and its subparts) relates to IA-7; CCI-000803}

For devices (including but not limited to [NIST FIPS 140-2](#) compliant radios) that have STIG/SRGs related to cryptographic module authentication (CCI-000803), comply with the requirements of those STIG/SRGs.

3.3 ACCESS CONTROL REQUIREMENTS

3.3.1 User Accounts

{For Government Reference Only: This subpart (and its subparts) relate to AC-2(a), AC-3, AC-6(1), AC-6(10), AC-6(2), AC-6(9), CM-11(2), and IA-2; CCI-002110, CCI-000213, CCI-001558, CCI-002221, CCI-002222, CCI-002223, CCI-002235, CCI-000039, CCI-001419, CCI-002234, CCI-001812, and CCI-000764. [For MODERATE Impact systems, this subpart \(and its subparts\) also relate to AC-2 \(2\), AC-2\(3\), AC-2\(4\), AC-6\(1\), and CM-5\(1\); CCI-001361, CCI-000017, CCI-000217, CCI-000018, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-001683, CCI-001684, CCI-001685, CCI-001686, CCI-002132, CCI-001558, CCI-002221, CCI-002222, CCI-002223, CCI-001813.](#)}

Any user interface supporting user accounts (either FULLY or MINIMALLY) must limit access according to specified limitations for each account. Install and configure any device having a STIG or SRG in accordance with that STIG or SRG.

All user interfaces FULLY supporting accounts must implement user-based authentication where each account is uniquely assigned to a specific user. User interfaces FULLY supporting accounts must implement at least three (3) levels of user account privilege including: 1) an account with read-only permissions 2) an account with full permissions including account creation and modification and 3) an account with greater permissions than read-only but without account creation and modification. Disable any unnecessary or unused accounts. Disable any "guest-level" accounts that are created on the system by default.

3.3.1.1 Computers

All computer operating systems must FULLY support user accounts and implement accounts for access. Each control system software application not supporting accounts and running on a computer must be installed such that use of the software is restricted by the computer operating system to specific users.

Applications running on computers must not require the user be logged in to a computer operating system administrator account for normal operation. It is permissible to require the computer operating system administrator account for initial application installation and configuration.

3.3.1.2 Controllers

For user interfaces provided by controllers, provide access control in accordance with the User Interface Requirements table for the applicable control system and user interface type.

- a. For table entries of "NA": NA means Not Applicable, there are no interfaces in this category.
- b. For table entries of "None Required": The user interface is not required to support user accounts.
- c. For table entries of "MINIMALLY": The user interface must at least MINIMALLY support user accounts.
- d. For table entries of "FULLY": The user interface must at FULLY support user accounts.
- e. For table entries of "KEY": The user interface must have physical security in the form of either a key lock on the interface itself or be furnished inside a lockable enclosure. Where this is required for a read only interface, the lockable enclosure must prevent viewing of data on the interface; for other interfaces, this lockable enclosure must prevent using the interface to alter data.
- f. For table entries of "Physical Security": For Local FULL interfaces, the interface must be located inside mission space. For Local Limited (not FULL) interfaces, the user interface must either a) be located within mission space or b) be protected by physical security at least as good as the control devices (and equipment controlled by the control devices) affected by the interface. For purposes of this requirement, 'affected' includes controllers with data that can be directly altered by the interface, as well as mechanical and/or electrical equipment directly controlled by those controllers, but does not include other interactions.
- g. Entries of the form "X and Y" must meet both the requirement indicated for X and the requirement indicated for Y. For example, an entry of "MINIMALLY and Physical Security" indicates the user interface must both MINIMALLY support accounts and have physical security.
- h. Entries of the form "X or Y" must meet either the requirement indicated for X or the requirement indicated for Y.

3.3.1.2.1 Fire Protection Systems

User Interface Requirements for MODERATE Impact Fire Protection Systems	
<u>User Interface Type</u>	<u>Access Control Requirement</u> (See note 2)
Local Read Only	None Required
Local Limited, Non-privileged	None Required
Local Limited, Privileged	KEY and Physical Security
Local Full	KEY
Remote Read Only	None Required
Remote Limited, Non-Privileged	FULLY
Remote Limited, Privileged AND Remote Full	FULLY
Notes: 1)Local Read Only User Interfaces are always Non-Privileged 2)Devices outside mission space require physical security protections as indicated (in "PHYSICAL SECURITY IN MODERATE IMPACT SYSTEMS")	

3.3.1.3 Additional User Account Expiration Requirements In MODERATE Impact Systems:

In addition to other user account requirements, user account expiration and auditing must be configured as indicated.

3.3.1.3.1 For Control System Applications Running on Computers

If temporary accounts are supported, expire temporary accounts 72 hours after creation. Expire all other accounts after 35 days of inactivity.

3.3.1.3.2 For Other Control System Devices FULLY Supporting Accounts

If temporary accounts are supported, expire temporary accounts 72 hours after creation. Expire all other accounts after 365 days of inactivity.

3.3.2 Unsuccessful Logon Attempts

{For Government Reference Only: This subpart (and its subparts) relate to AC-7 (a), AC-7 (b); CCI-000043, CCI-000044, CCI-001423, CCI-002236, CCI-002237, CCI-002238}

Except for high availability user interfaces indicated as exempt, devices must meet the indicated requirements for handling unsuccessful logon attempts. If a device cannot meet these requirements, document device capabilities to protect from subsequent logon attempts and propose alternate protections in a [Device Account Lock Exception Request](#) submittal. Do not implement alternate protection measures in lieu of the indicated requirements without explicit permission from the Government. If no Device Account Lock Exceptions are requested, provide a document stating that no approval is being requested as the Device Account Lock Exception Request.

3.3.2.1 Devices MINIMALLY Supporting Accounts

For MODERATE Impact Systems: Devices which MINIMALLY (but not FULLY) support accounts must lock the user account after five minutes and must unlock the user account after 60 minutes have elapsed without an unsuccessful login attempt or by a successful login to a separate administrator account.

3.3.2.2 Devices FULLY Supporting Accounts

Devices which FULLY support accounts must meet the following requirements.

- a. It must lock the user account when three unsuccessful logon attempts occur within a 15 minute interval.
- b. Once an account is locked, the account must stay locked until unlocked by an administrator. If the account being locked is the sole administrator account on the device, the account must stay locked for 1 hour and then automatically unlock.
- c. Once the indicated number of unsuccessful logon attempts occurs, delay further logon prompts by 5 seconds.

3.3.2.3 High Availability Interfaces Exempt from Unsuccessful Logon Attempts Requirements

There are no high availability interfaces which are exempt from unsuccessful logon attempts requirements.

3.3.3 System Use Notification

{For Government Reference Only: This subpart (and its subparts) relates to AC-8; CCI-000048, CCI-002247, CCI-002243, CCI-002244, CCI-002245, CCI-002246, CCI-000050, CCI-002248}

3.3.3.1 System Use Notification for Remote User Interfaces

Remote user interfaces must display a warning banner meeting the requirements of DTM 08-060 on screen.

3.3.3.2 System Use Notification for Local User Interfaces

Devices which are connected to a network and have a local user interface must display a warning banner meeting the requirements of DTM 08-060 on the user interface screen if capable of doing so and must have a permanently affixed label with an approved banner from DTM 08-060 if unable to display the warning banner on the screen. Where it is impractical (perhaps due to device size) to affix the label to the device, affix the label to the device enclosure.

Labels must be machine printed or engraved, plastic or metal, designed for permanent installation, must use a font no smaller than 14 point, and must provide a high contrast between font and background colors.

3.3.4 Session Lock and Session Termination Requirements In MODERATE Impact Systems:

{For Government Reference Only: This subpart (and its subparts) relates to AC-11(a), AC-11(b), AC-11(1), AC-12, SC-10; AC-10; CCI-000058, CCI-000059, CCI-000056, CCI-000057, CCI-000060, CCI-002360, CCI-002361, CCI-001133, CCI-001134, CCI-000054, CCI-000055, CCI-002252}

3.3.4.1 Session Termination

When session termination is required for a User Interface, the User Interface must implement session termination a) based on manual initiation, or b) based on lack of activity, or c) based on either manual initiation or lack of activity, as indicated.

Session Termination must result in logging out the user. A logged out User Interface may only perform actions as indicated in the "Permitted Actions Without Identification or Authentication" subpart of this Section or display a publicly viewable image or blank screen. User Interfaces must remain logged out (session terminated) until a user enters correct authentication information, which must initiate a new session. All User Interfaces running on computers and all Remote User Interfaces must also terminate network connections as part of session termination.

3.3.4.2 Session Lock

When session lock is required for a User Interface, the User Interface must implement session lock a) based on manual initiation, or b) based on lack of activity, or c) based on either manual initiation or lack of activity, as indicated.

Session lock must result in the User Interface being suspended and the user interface must display a publicly viewable image or blank screen. No interaction with the user interface must be possible until either a) the same user enters valid authentication information, in which case that session must be continued, or b) until a different user enters valid authentication information at which point the first session must be terminated and a new session initiated for the new user.

3.3.4.3 Session Lock and Termination for Computers

Except as shown in the Session Lock and Session Termination Exception Table, User Interface sessions provided by computer operating systems must support the requirement for both Session Lock and Session Termination. Session Lock and Session Termination must be capable of being initiated by the user and must also be initiated by lack of activity. Session Lock must occur after 15 minutes of inactivity, and Session Termination must occur after 30 minutes total of inactivity (including, not in addition to, the time for Session Lock). When a user initiates a new session, terminate existing sessions if necessary to limit the total number of concurrent sessions to 1.

Other User Interface sessions running on computers (for local user interfaces) or hosted on a computer (for remote user interfaces) and supporting accounts must support user initiation of Session Termination and session lock. Session lock may be initiated by user initiation or automatically after 15 minutes of inactivity. In addition, remote User Interface sessions must also initiate Session Termination after 30 minutes of inactivity unless otherwise indicated in the Session Lock and Termination Exceptions table.

3.3.4.4 Session Lock and Termination for Controllers

Writable Remote User Interfaces must support requirements for Session Termination, and must both be capable of being initiated by the user and initiated by lack of activity. Session Termination must initiate after 30 minutes of inactivity.

Except as shown in the Session Lock and Session Termination Exception Table, Local User Interfaces supporting accounts must support manual initiation of Session Termination. Privileged Local User Interfaces must also support timed initiation of Session Termination, unless otherwise indicated in the Session Lock and Termination Exceptions table, with Session Termination initiated at 30 minutes of inactivity. They must also support session lock, where session lock may be initiated by user initiation or automatically after 15 minutes of inactivity.

3.3.5 Permitted Actions Without Identification or Authentication

{For Government Reference Only: This subpart (and its subparts) relates to AC-14; CCI-000061, CCI-000232}

The control system must require identification and authentication before allowing any actions except read-only actions by a user acting from a user interface which MINIMALLY or FULLY supports accounts.

3.3.6 Physical Security in MODERATE Impact Systems

{For Government Reference Only: This subpart relates to PE-3(1), PE-4, PE-5, SC-7(a), SC-7(c), SC-8, SC-8(1); CCI-000928, CCI-002926, CCI-000936, CCI-002930, CCI-002931, CCI-000937, CCI-001097, CCI-001109, CCI-002418, CCI-002419, CCI-002421.}

3.3.6.1 Physical Security for Media

3.3.6.1.1 Physical Security for Media Inside Mission Space

Install all non-IP network media located inside of the mission space in conduit. Install all IP network media located inside of the mission space in intermediate metallic conduit.

3.3.6.1.2 Physical Security for Media Outside Mission Space

Install all network media (both IP and non-IP) located outside of the mission space in rigid metallic conduit.

3.3.6.1.3 Physical Security for Non-Network Media in Fire Protection Systems

For Fire Suppression Systems which can be inhibited or forced to activate by manipulation of non-network wiring, install all non-network media outside of mission space, including analog and binary instrumentation wiring and power wiring, in rigid metallic conduit.

3.3.6.2 Physical Security for Devices

Install all devices (computers and controllers) which are located outside of mission space in lockable enclosures. (Recall that per definition of mission space, a room controlled by the mission is mission space regardless of whether it is contiguous with other mission space.)

Install all controllers connected to an IP network in lockable enclosures (both inside and outside of mission space).

3.3.6.2.1 Physical Security for Devices in Fire Protection Systems

For Fire Suppression systems with a release panel, install all components of the suppression system either inside mission space, or within locked enclosures. Components of these systems include: release panel, any relay or interface panels, analog and binary inputs or outputs, control valves, manual valves.

3.3.6.3 Physical Security for User Interfaces

Physical security requirements for User Interfaces are specified in the preceding paragraphs of this Section.

3.3.7 Enclosures

Prior to final acceptance of the system, lock all lockable enclosures. Submit an [Enclosure Keys](#) submittal with all copies of keys for all enclosures and a key inventory list documenting all keys. Label each key with the matching enclosure identifier.

3.4 USER IDENTIFICATION AND AUTHENTICATION

{For Government Reference Only: This subpart (and its subparts) relates to IA-2, IA-2(1), IA-2(12), IA-5 IA-5(b), IA-5(c), IA-5(e), IA-5(g), IA-5(1), IA-5(11); CCI-000764, CCI-000765, CCI-001953, CCI-001954, CCI-001544, CCI-001989, CCI-000182, CCI-001610, CCI-000192, CCI-000193, CCI-000194, CCI-000205, CCI-001619, CCI-001611, CCI-001612, CCI-001613, CCI-001614, CCI-000195, CCI-001615, CCI-000196, CCI-000197, CCI-000199, CCI-000198, CCI-001616, CCI-001617, CCI-000200, CCI-001618, CCI-002041, CCI-002002, CCI-002003. For MODERATE

Impact systems, this subpart also relates to AC-6 (1), AC-6(10), AC-6(2), AC-6(9)IA-2(4), IA-5(13); CCI-001558, CCI-002221, CCI-002222, CCI-002223, CCI-002235, CCI-000039, CCI-001419, CCI-002234, CCI-000768, CCI-002007.}

This subpart indicates requirements for specific methods of identification and authentication for users and user accounts. Where these requirements conflict apply the following order of precedence: 1) If present, Device Specific Requirements take precedence over any other requirements; and then 2) multifactor authentication requirements take precedence over password requirements.

3.4.1 User Identification and Authentication for All System Types

Unless otherwise indicated, all user interfaces supporting accounts (either FULLY or MINIMALLY) must implement Identification and Authorization via passwords.

For MODERATE Impact Systems: User interfaces provided by computer operating systems must implement multifactor authentication via PIV. Software running on computers and computer operating systems must manage cached authenticators in accordance with the relevant STIGs. All other devices and software must not use cached authenticators.

3.4.2 User Identification and Authentication for Specific System Types

System specific requirements are in addition to and supersede those indicated for all system types. When no additional requirements are indicated for a specific system type the requirements for all systems still apply to that system type.

3.4.3 User Identification and Authentication for Specific Devices

There are no additional device specific user interface requirements

3.4.4 Implementation of Identification and Authorization Requirements

Identification and Authorization must be met by one of the following methods:

- a. Direct implementation in the user interface.
- b. For user interfaces on a computer: inheriting the Identification and Authorization from the computer operating system, either by the operating system limiting access to specific applications by user, or by the application itself having permissions based on the user logged into the computer.
- c. For remote interfaces: an implementation shared between the remote user interface server and the remote user interface client. For example, a requirement for PIV authentication may be met on a remote user interface by a PIV reader on a web browser client which sends the authentication information via HTTPS to the remote server.

3.4.5 Password-Based Authentication Requirements

3.4.5.1 Passwords for Software and Applications Running on Computers

All software and applications running on computers supporting password-based authentication must enforce the following requirements:

- a. Minimum password length of 12 characters
- b. Password must contain at least one uppercase character.
- c. Password must contain at least one lowercase character.
- d. Password must contain at least one numeric character.

- e. Password must contain at least one special character. The list of supported special characters must include at least 4 separate characters.
- f. Password must have a minimum lifetime of 24 hours.
- g. Password must have a maximum lifetime of 60 days. When passwords expire, prompt users to change passwords. Do not lock accounts due to expired passwords.
- h. Password must differ from previous five passwords, where differ is defined as changing at least 50 percent of the characters (where location is significant, a character may be reused if it is in a different position).
- i. Passwords must be cryptographically protected during storage and transmission.

3.4.5.2 Passwords for Controllers FULLY Supporting Accounts

All controllers FULLY supporting accounts and supporting password-based authentication must enforce the following requirements:

- a. Minimum password length of 12 characters
- b. Password must contain at least one uppercase character.
- c. Password must contain at least one lowercase character.
- d. Password must contain at least one numeric character.
- e. Password must contain at least one special character. The list of supported special characters must include at least 4 separate characters.
- f. Password must have a maximum lifetime of sixty (60) days. When passwords expire, prompt users to change passwords. Do not lock accounts due to expired passwords.
- g. Password must differ from previous five passwords, where differ is defined as changing at least 50 percent of the characters.
- h. Passwords must be cryptographically protected during storage and transmission.

3.4.5.3 Passwords for Remote Interfaces

Passwords for connecting to a Remote User Interface supporting password-based authentication must enforce the following requirements:

- a. Minimum password length of 12 characters
- b. Password must contain at least one uppercase character.
- c. Password must contain at least one lowercase character.
- d. Password must contain at least one numeric character.
- e. Password must contain at least one special character. The list of supported special characters must include at least 4 separate characters.
- f. Password must have a maximum lifetime of 60 days. When passwords expire, prompt users to change passwords. Do not lock accounts due to expired passwords.
- g. Password must differ from previous five passwords, where differ is defined as changing at least 50

percent of the characters (where location is significant, a character may be reused if it is in a different position).

h. Passwords must be cryptographically protected during storage and transmission.

3.4.5.4 Passwords for Devices Minimally Supporting Accounts

Devices MINIMALLY supporting accounts must support passwords with a minimum length of four characters.

3.4.5.5 Password Configuration and Reporting

For all devices with a password, change the password from the default password. Coordinate selection of passwords with the Password Point of Contact. Do not use the same password for more than one device unless specifically instructed to do so. Provide a [Confidential Password Report](#) documenting the password for each device and describing the procedure to change the password for each device.

Do not provide the Password Summary Report in electronic format. Provide two hardcopies of the Password Summary Report, each copy in its own sealed envelope.

3.4.6 Authenticator Feedback

{For Government Reference Only: This subpart relates to IA-6; CCI-000206}

Devices must never show authentication information, including passwords, on a display. Devices that momentarily display a character as it is entered, and then obscure the character, are acceptable. For devices that have STIGs or SRGs related to obscuring of authenticator feedback (CCI-000206), comply with the requirements of those STIGS/SRGs.

3.4.7 Implementation of PKI Infrastructure in Moderate Impact Systems

Coordinate with the PKI Infrastructure Point of Contact to configure the system to implement PKI such that the system validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information; the system enforces authorized access to the corresponding private key; the system maps the authenticated identity to the account of the individual or group; and the system implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.

3.5 CYBERSECURITY AUDITING

Where an auditing requirement exists for email notification, notify via email the application administrator and Information System Security Officer (ISSO) of the event. Coordinate with the Email Address Point of Contact for email addresses. If outgoing email is not available to the system, disable email notifications.

3.5.1 Audit Events, Content of Audit Records, and Audit Generation

{For Government Reference Only: This subpart (and its subparts) relates to AU-2(a), AU-2(c), AU-2(d), AU-3, AU-10, AU-12, AU-14(b), AU-14(1), AU-14(2), AU-14(3), CM-5(1), SC-7 (9); CCI-000123, CCI-001571, CCI-000125, CCI-001485, CCI-000130, CCI-000131, CCI-000132, CCI-001230, CCI-000133, CCI-000134, CCI-001487, CCI-000166, CCI-001899, CCI-000169, CCI-001459, CCI-000171, CCI-000172, CCI-001910, CCI-001914, CCI-001919, CCI-001464, CCI-001462, CCI-001920, CCI-001814, CCI-002400. For MODERATE Impact systems, this subpart (and its subparts) also relates to AU-3 (1); CCI-000135, CCI-001488}

For devices that have STIG/SRGs related to audit events, content of audit records or audit generation, comply with the requirements of those STIG/SRGs.

If auditing requirements can be met using existing control system alarm or event capabilities, those existing capabilities may be used to meet these requirements.

3.5.1.1 Computers

For each computer, provide the capability to select audited events and the content of audit logs. Configure computers to audit the indicated events, and to record the indicated information for each auditable event. Send logs to a syslog server that is only accessible via accounts on the system with privileged level access.

3.5.1.1.1 Audited Events

Configure each computer to audit the following events:

- a. Successful and unsuccessful attempts to access, modify, or delete privileges, security objects, security levels, or categories of information (e.g. classification levels)
- b. Successful and unsuccessful logon attempts
- c. Successful logouts
- d. Privileged activities or other system level access
- e. Concurrent logons from different workstations
- f. Successful and unsuccessful accesses to objects
- g. Program initiations
- h. Direct access to the information system
- i. Account creations, modifications, disabling, and terminations. **For MODERATE Impact Systems, also provide email notification when these audit events occur.**
- j. Kernel module load, unload, and restart

3.5.1.1.2 Audit Event Information To Record

Configure each computer to record, for each auditable event, the following information (where applicable to the event):

- a. What type of event occurred
- b. When the event occurred
- c. Where the event occurred
- d. The source of the event
- e. The outcome of the event
- f. The identity of any individuals or subjects associated with the event
- g. **For MODERATE Impact Systems: For all privileged commands, full-text recording of the executed command and the user executing the command**

For MODERATE Impact Systems: Audit records must provide sufficient detail to reconstruct events to determine cause of compromise and magnitude of damage, malfunction, or security violation.

3.5.2 Audit Time Stamps

{For Government Reference Only: This subpart (and its subparts) relates to AU-8; CCI-000159, CCI-001889, CCI-001890. For MODERATE Impact systems, this subpart (and its subparts) also relates to AU-8 (1); CCI-001891, CCI-001892, CCI-002046.}

Any device (computer or controller) generating audit records must have an internal clock capable of providing time with a resolution of one second. Clocks must not drift more than 10 seconds per day. Configure the system so that each device (computer or controller) generating audit records maintains accurate time to within 1 second. Note that if the control system specifications include requirement for clocks, the most stringent requirement applies.

3.5.3 Auditing Front End Software

The project site currently has the following software to support control system auditing: none. If there is no existing auditing front end software or the software is not compatible with the provided control systems, provide Auditing Front End Software with audit log import and upload, export, notification, and analysis functionality. The Auditing Front End Software may be provided as a component of the control system front end or as a separate software package, and a single package may serve multiple control systems provided under the same projects if they are sharing a cybersecurity authorization.

When the Auditing Front End Software is neither existing nor installed under the requirements of another Section, furnish the Auditing Front End Software media and license for subsequent Government installation and install the software on TBD. Submit copies of Auditing Front End Software if this function is not part of the software provided with the control system to meet requirements of other Sections.

3.5.3.1 Import and Upload Requirements

Auditing Front End Software must be capable of importing audit logs from the Device Audit Record Upload Software and of uploading audit logs over the network from all control system devices supporting network upload of audit logs.

3.5.3.2 Export Requirements

Auditing Front End Software must be capable of exporting to a file format supported by Microsoft Excel.

3.5.3.3 Notification Of Audit Failure in Devices in MODERATE Impact Systems

The auditing front end software must be capable of receiving notifications of audit failure from control system devices and computers and be able to provide email notification based on receipt of the notification.

3.5.3.4 Audit Reduction and Report Generation In MODERATE Impact Systems

{For Government Reference Only: This subpart (and its subparts) relates to AU-6(4), AU-7(a), AU-7(b), AU-7(1), AU-12(1); CCI-000154, CCI-001875, CCI-001876, CCI-001877, CCI-001878, CCI-001879, CCI-001880, CCI-001881, CCI-001882, CCI-000158, CCI-000173, CCI-000174, CCI-001577.}

Auditing Front End Software must provide audit reduction and reporting capabilities that supports on-demand review and analysis, on demand reporting, and after the fact investigations of security incidents. The software must be able to combine audit records from all components within the system and analyze them as a single audit record. The software must correct for discrepancies in timestamps of audit logs from different sources and be able to account for discrepancies up to 2 seconds between sources. The software must not alter original audit record content or time ordering of audit records. The software must have the capability to filter audit records using user-defined fields within the audit records.

The audit reduction and reporting capabilities may incorporate third party application, such as Excel or Access.

3.5.4 Audit Storage Capacity and Audit Upload

{For Government Reference Only: This subpart (and its subparts) relates to AU-4; CCI-001848, CCI-001849}

The creation of audit records must never interfere with normal device operation. Devices must cease collection of auditing information if required to maintain normal operation.

- a. For devices that have STIG/SRGs related to audit storage capacity (CCI-001848 or CCI-001849) comply with the requirements of those STIG/SRGs.
- b. For controllers capable of generating audit records, provide 60 days worth of secure local storage, assuming 10 auditable events per day.

3.5.4.1 Audit Log Storage Notification In MODERATE Impact Systems

{For Government Reference Only: This subpart (and its subparts) relates to AU-5(1); CCI-001855.}

Controllers storing audit logs must provide notification when audit logs reach 75 percent of capacity either directly through email or indirectly by sending a notification to a computer, and the computer sending an email. Computers storing audit logs must provide notification when audit logs reach 75 percent of capacity directly through email.

3.5.4.2 Device Audit Record Upload Software

For each device (computer or controller) required to audit events and for which audit logs cannot be uploaded over the network by the Auditing Front End Software, provide and license to the Government software implementing a secure mechanism of uploading audit records from the device and exporting them to the Auditing Front End Software. Where different devices use different software, provide software of each type required to upload audit logs from all devices.

When Device Audit Record Upload Software is capable of uploading audit logs over the network, install Device Audit Record Upload Software on the same computer as the Auditing Front End Software. Submit copies of device audit record upload software if this function is not part of the software provided with the control system to meet requirements of other Sections. If there are no devices requiring this software, provide a document stating this in lieu of this submittal.

3.5.5 Response to Audit Processing Failures

{For Government Reference Only: This subpart (and its subparts) relates to AU-5; CCI-000139, CCI-000140, CCI-001490.}

In the case of a failure in the auditing system, computers associated with auditing must provide email notification. For MODERATE Impact systems, the computer must also notify the associated auditing front end software. In case of an audit failure, if possible, continue to collect audit records by overwriting existing audit records.

For MODERATE Impact Systems: In the case of an audit failure at a controller performing auditing, the device must notify the associated auditing front end software of the audit failure if able, and must continue to collect audit records by overwriting existing audit records if able. The auditing front end software must provide notification as indicated, treating the notification of failure from the device as a failure in the auditing system.

3.6 REQUIREMENTS FOR LEAST FUNCTIONALITY

{For Government Reference Only: This subpart (and its subparts), along with the Network Communication, Ports, Protocols and Services Report submittal specified elsewhere in this section, relates to CM-6(a), CM-6(c), CM-7, CM-7(1)(b), SC-41; CCI-000363, CCI-000364, CCI-000365, CCI-001588, CCI-001755, CCI-000381, CCI-000380, CCI-000382, CCI-001761, CCI-001762, CCI-002544, CCI-002545, CCI-002546. For MODERATE Impact systems, this subpart (and its subparts) also relates to CM-7(2), CM-7(5)(a), CM-7(5)(b); CCI-000381, CCI-000380, CCI-000382, CCI-001761, CCI-001762}

For devices that have a STIG or SRG related to Requirements for Least Functionality (such as configuration settings and port and device I/O access for least functionality), install and configure the device in accordance with that STIG or SRGs.

3.6.1 Device Capabilities

Do not provide devices with remote user interfaces or full user interfaces where one was not required. Do not use a networked sensor or actuator where a non-networked sensor or actuator would suffice.

For all MODERATE Impact Systems: Unless specifically required by the government, do not provide a capability to update device firmware over the network.

3.6.2 Software

For software that has a STIG or SRG related to Requirements for Least Functionality (such as configuration settings and port access for least functionality), install and configure the software in accordance with that STIG or SRG.

Do not install software that is not specifically required to meet a contract requirement. Remove any previously installed that is not specifically required to meet a contract requirement. Do not implement functionality within software that is not specifically required to meet contract requirements.

3.7 SYSTEM AND COMMUNICATION PROTECTION

3.7.1 Collaborative Computing

{For Government Reference Only: This subpart relates to SC-15(a), SC-15(b); CCI-001150, CCI-001152.}

Without explicit approval from the project site, control systems must not use collaborative computing technologies.

3.7.2 Denial of Service Protection and Application Partitioning In MODERATE Impact Systems:

{For Government Reference Only: This subpart relates to SC-5, SC-12, SC-7(a); CCI-001093, CCI-002385, CCI-002386, CCI-002430, CCI-001097. For MODERATE Impact systems, this subpart also relates to SC-2; CCI-001082.}

To the greatest extent practical, implement control logic without reliance on the network. Except when required to meet the requirements of the control system Section (where the requirement can only be met using computer hardware), do not implement control logic in computers. For MODERATE Impact systems, do not implement control logic in a device providing (i.e. acting as a server for) a Full Remote User Interface.

3.7.2.1 Default Requirements for MODERATE Impact Control Systems

Except for networked input and outputs on input-output buses specifically designed to provide high

reliability or redundancy, sensors and actuators must not rely on the network to exchange data with the controller executing the sequence of operation which uses the sensor value or determines the actuator command.

Sensor values required by multiple devices may be shared over the network provided they are connected to a controller requiring the value for execution of the sequence and that controller shares the value on the network.

3.7.3 Mobile Code In MODERATE Impact Systems:

{For Government Reference Only: This subpart relates to SC-18(a), SC-18(b), SC-18(c), SC-18(1), SC-18(3), SC-18(4); CCI-001160, CCI-001161, CCI-001162, CCI-001163, CCI-001164, CCI-001165, CCI-001166, CCI-001662, CCI-002457, CCI-002458, CCI-001169, CCI-001695, CCI-001170, CCI-002469}

Devices with STIGs/SRGs related to Mobile Code and to Security Control SC-18 must be installed in accordance with the relevant STIGs/SRGs. All remote user interfaces must meet the requirements of the "Web Browsers and Application SRG".

Mobile code may only be downloaded from a specifically authorized mobile code repository. Coordinate with the Mobile Code Point of Contact for the location of a repository.

3.7.4 Protection of Information at Rest In MODERATE Impact Systems:

{For Government Reference Only: This subpart relates to SC-28, SC-28(1); CCI-001199, CCI-002472, CCI-002475, CCI-002476}

Computers must protect information at rest in accordance with applicable STIGs.

Any control system device storing personally identifiable information (PII), controlled unclassified information (CUI), or classified information must be protected by an Information At Rest encryption solution or by a physical security solution. Provide a [Protection of Information At Rest Proposal](#) indicating each device storing PII, CUI, or classified information and the encryption or physical security solution proposed for that device for government approval. If no devices stores PII, CUI, or classified information, provide a document stating this as the Protection of Information At Rest Proposal submittal. Do proceed with device selection and installation until the Protection of Information At Rest Proposal is approved. Once approved, implement approved Information At Rest protections.

3.7.5 Process Isolation and Boundary Protection in Moderate Impact Fire Protection Systems

{For Government Reference Only: This subpart relates to SC-7(a), SC-7(c), SC-7(4)(a), SC-7(4)(c), SC-7(5), SC-7(7), SC-7(9)(a), SC-7(11), SC-7(13), SC-7(13), SC-7(18); CCI-001097, CCI-001098, CCI-001102, CCI-002396, CCI-001109, CCI-002397, CCI-002398, CCI-002399, CCI-002403, CCI-001120, CCI-001119, CCI-001126}

3.7.5.1 Radio Interfaces for Fire Protection Systems

When radios interfacing a local fire protection system to a supervisory system are not [NIST FIPS 140-2](#) validated, use a relay panel interface between the local fire protection system and the radio. Install and configure the relay panel to prohibit initiating any action within the local fire protection system other than causing the system to play a pre-recorded message or causing the system to play a live audio message. Install relays using the normally open contact such that they pass a signal when they close, and so that a relay that loses power or has a failed coil does not pass a signal

3.7.5.2 Fire Suppression System Network Isolation

For fire suppression systems including a release panel, any network used in these systems must be dedicated to these systems and must be isolated from any other network, including other components

of the Fire Alarm and Fire Suppression systems. Use only dry contacts and relays to transfer signals from these systems to any other systems. Install relays using the normally open contact such that they pass a signal when they close, and so that a relay that loses power or has a failed coil does not pass a signal

3.8 SAFE MODE AND FAIL SAFE OPERATION

{For Government Reference Only: This subpart (and its subparts) relates to CP-12, SI-10(3), SI-17; CCI-002855, CCI-002856, CCI-002857, CCI-002754, CCI-002773, CCI-002774, CCI-002775}

For all control system components with an applicable STIG or SRG, configure the component in accordance with all applicable STIGs and SRGs.

3.9 SYSTEM MAINTENANCE TOOL SOFTWARE

{For Government Reference Only: This subpart (and its subparts) relates to MA-3; CCI-000865.}

Submit and license to the Government all software required to operate, maintain and modify the control system such the Government or their agents are able to perform repair, replacement, upgrades, and expansions of the system without subsequent or future dependence on the Contractor, Vendor or Manufacturer. Submit hard copies of user manuals for each software with the software submittal. Provide any hardware keys or dongles, software keys, license numbers, and other information required to enable the Government to access or change the system.

For software provided and licensed to the Government under the requirements of another Section, submit a statement indicating the Section and Submittal under which the software was provided. For software provided to meet the requirements of this Section and not provided and licensed under another Section, submit software and software user manuals on DVD or CD as a Technical Data Package and submit one hard copy of the software user manual for each piece of software.

3.10 DEVICE POWER

{For Government Reference Only: This subpart (and its subparts) relates to PE-11, PE-11(1); CCI-002955, CCI-000961. For MODERATE Impact systems, this subpart (and its subparts) also relates to PE-9, PE-9(1); CCI-000952, CCI-002953, CCI-002954.}

For MODERATE Impact Systems: Provide control system with power supply meeting or exceeding the reliability of the controlled equipment. Powering control system devices using the same power source as the equipment controlled by the device is a permissible method of meeting this requirement. Without explicit approval from the government, do not install local uninterruptible power supplies (UPSes) as a source of device power.

3.10.1 Device Behavior on Loss of Power In MODERATE Impact Systems:

Application programs and configuration settings must be stored in devices in manner such that a loss of power does not result in a loss of the application program or configuration settings: Loss of power must never result in the loss of application programs, regardless of the length of time power is lost; and loss of power for less than 2,500 hours must not result in the loss of configured settings.

In the event of a loss of power, when power is restored, controllers and computers executing control logic (and the underlying equipment) must recover and resume their normal sequences of operation. Note that the sequence of operation may require specific actions (e.g. startup sequences) upon recovery from loss of power.

3.11 VULNERABILITY SCANNING

{For Government Reference Only: This subpart (and its subparts) relates to RA-5 RA-5(a),RA-5(b),RA-5(c),RA-5(d); CCI-001054, CCI-001055, CCI-000156, CCI-001641, CCI-001643, CCI-001057, CCI-001058, CCI-001059. For MODERATE Impact systems, this subpart (and its

subparts) also relates to RA-5(1), RA-5(5); CCI-001062, CCI-001067, CCI-001645, CCI-002906.}

All IP devices must be scannable, such that the device can be scanned by industry standard IP network scanning utilities without harm to the device, application, or functionality.

3.11.1 Computers and Software Running on Computers

Computers and applications running on computers must meet relevant vulnerability scanning STIGs/SRGs and respond to approved DoD vulnerability scanning tools.

3.11.2 Controllers

Provide controllers that are scannable by standard control system discovery tools or control system browsers and return meaningful status information including the network inputs and outputs for the controller. This information must contain sufficient detail to detect vulnerabilities or exploits of the controller.

Provide all software needed to scan the control system as the [Control System Scanning Tools](#) submittal. If the software required to scan the system is already installed at the project site or is provided under a separate section instead provide a statement indicating this.

3.12 SYSTEM AND INTEGRATION INTEGRITY

3.12.1 Malicious Code Protection

{For Government Reference Only: This subpart (and its subparts) relates to SI-3(c); CCI-001241, CCI-002623}

For all computers installed under this project, provide malware protection software media, provide licenses, and install and configure malware protection software as indicated. Coordinate with the Government Computer Access Point of Contact as required.

- a. Provide malware protection software licenses.
- b. Provide malware protection software media.
- c. Install and configure malware protection software in accordance with the relevant STIGs.

3.12.2 Software, Firmware, and Information Integrity In MODERATE Impact Systems:

{For Government Reference Only: This subpart relates to CM-5(3); CCI-001749, CCI-002704, CCI-002726}

If there exists [Integrity Verification Software](#) that can check boot process, software, firmware, or information in the control system and verify its integrity, provide it. If no such software exists, provide a statement to this affect in lieu of the software.

The system prevents the installation of software and firmware without verification of the digital signature using an approved certificate.

3.13 CONTROL SYSTEM CYBERSECURITY TESTING

{For Government Reference Only: For MODERATE Impact systems, this subpart (and its subparts) relates to SA-11(a), SA-11(b), SA-11(c), SA-11(d), SA-11(e); CCI-003171, CCI-003172, CCI-003173, CCI-003174, CCI-003175, CCI-003176, CCI-003177, CCI-003178.}

3.13.1 Control System Cybersecurity Testing Procedures

Prepare and submit Control System Cybersecurity Testing Procedures explaining step-by-step, the actions and expected results that will demonstrate that the control system meets the requirements of this Section. The Control System Cybersecurity Testing Procedures may be submitted as a Technical Data Package.

3.13.2 Control System Cybersecurity Testing Execution

Using the Control System Cybersecurity Testing Procedures verify that the control system meets the requirements of this Section. **UNLESS GOVERNMENT WITNESSING OF A TEST IS SPECIFICALLY WAIVED BY THE GOVERNMENT, PERFORM ALL TESTS WITH A GOVERNMENT WITNESS.** If testing reveals deficiencies in the system, correct the deficiency and retest until successful.

3.13.3 Control System Cybersecurity Testing Report

Prepare and submit a Control System Cybersecurity Testing Report documenting all tests performed and their results. Include all tests in the Control System Cybersecurity Testing Procedures and any additional tests performed during testing. Document test failures and repairs conducted with the test results. The Control System Cybersecurity Testing Report may be submitted as a Technical Data Package

3.14 FIELD QUALITY CONTROL, CYBERSECURITY VALIDATION SUPPORT

AM0003* In addition to testing and testing support required by other Sections, provide a minimum of ~~420~~¹⁶ hours of technical support for cybersecurity testing of control systems to support the DoD Risk Management Framework process Cybersecurity assessment of the control system. This support is independent of (and in addition to) the Control System Cybersecurity Testing specified in this section.

***AM0003**

3.15 CYBERSECURITY TRAINING

Provide eight hours of classroom and hands-on training for six Government personnel on the cybersecurity operation and maintenance of the control system provided. This training is in addition to and must be coordinated with control system training specified in other Sections.

The Government will provide the training location. Training must cover, at a minimum: (a) applying software and firmware updates, (b) user account creation, modification and deletion, (c) audit log upload procedures and (d) identification of privileged user interfaces and system impact of those interfaces. Training session must include a question and answer period during which government staff questions about cybersecurity aspects of the control system are answered.

-- End of Section --

SECTION TABLE OF CONTENTS

DIVISION 25 - INTEGRATED AUTOMATION

SECTION 25 05 11.04

CYBERSECURITY FOR FACILITY-RELATED CONTROL SYSTEMS: LIGHTING CONTROL SYSTEM

PART 1 GENERAL

- 1.1 CONTROL SYSTEM APPLICABILITY
- 1.2 RELATED REQUIREMENTS
- 1.3 REFERENCES
- 1.4 DEFINITIONS
 - 1.4.1 Administrator Account
 - 1.4.2 Computer
 - 1.4.3 Controller
 - 1.4.4 Mission Space
 - 1.4.5 Network
 - 1.4.6 Network Connected
 - 1.4.6.1 Wireless Network Connected
 - 1.4.7 Network Media
 - 1.4.8 User Account Support Levels
 - 1.4.8.1 FULLY Supported
 - 1.4.8.2 MINIMALLY Supported
 - 1.4.8.3 NOT Supported
 - 1.4.9 Manual Local Input
 - 1.4.10 Card Reader
 - 1.4.11 User Interface
 - 1.4.11.1 Local User Interface
 - 1.4.11.2 Remote User Interface
 - 1.4.11.3 Types of User Interface (by capability)
 - 1.4.11.3.1 Read-Only User Interface
 - 1.4.11.3.2 Limited User Interface
 - 1.4.11.3.3 Full User Interface
 - 1.4.11.3.4 View-Only User Interface
 - 1.4.11.4 Other User Interface Terminology
 - 1.4.11.4.1 Writable User Interface
 - 1.4.11.4.2 Privileged User Interface
 - 1.4.12 Wireless Network
 - 1.4.13 Wired Broadcast Network
- 1.5 ADMINISTRATIVE REQUIREMENTS
 - 1.5.1 Points of Contact
 - 1.5.2 Coordination
- 1.6 SUBMITTALS
- 1.7 CYBERSECURITY DOCUMENTATION
 - 1.7.1 Proposed STIG and SRG Applicability Report
 - 1.7.2 Cybersecurity Interconnection Schedule
 - 1.7.3 Network Communication, Ports, Protocols and Services Report
 - 1.7.4 Control System Inventory Reports
 - 1.7.5 Software and Configuration Backups
 - 1.7.6 Cybersecurity Network (Riser) Diagram
 - 1.7.7 STIG, SRG and Vendor Guide Compliance Result Report
 - 1.7.8 Control System Cybersecurity Documentation

- 1.7.8.1 Software Applications
- 1.7.8.2 For Lighting Control System Devices
 - 1.7.8.2.1 Lighting Control System Devices FULLY Supporting User Accounts
 - 1.7.8.2.2 All Other Lighting Control System Devices
- 1.8 SOFTWARE LICENSING
- 1.9 CYBERSECURITY DURING CONSTRUCTION
 - 1.9.1 Contractor Computer Equipment
 - 1.9.1.1 Operating System
 - 1.9.1.2 Anti-Malware Software
 - 1.9.1.3 Passwords and Passphrases
 - 1.9.1.4 User-Based Authentication
 - 1.9.1.5 Demonstration of Compliance
 - 1.9.1.6 Contractor Computer Cybersecurity Compliance Statements
 - 1.9.2 Temporary IP Networks
 - 1.9.2.1 Network Boundaries and Connections
 - 1.9.3 Government Access to Network
 - 1.9.4 Passwords and Passphrases
 - 1.9.5 Contractor Temporary Network Cybersecurity Compliance Statements
- 1.10 CYBERSECURITY DURING WARRANTY PERIOD

PART 2 PRODUCTS

- 2.1 ETHERNET SWITCH
 - 2.1.1 Required Functionality
 - 2.1.2 Configuration Requirements
- 2.2 DAISY CHAIN IP CONTROLLERS

PART 3 EXECUTION

- 3.1 CYBERSECURITY HARDENING AND CONFIGURATION GUIDES
- 3.2 NETWORK REQUIREMENTS
 - 3.2.1 Wireless and Wired Broadcast Communication
 - 3.2.1.1 Wireless and Wired Broadcast IP Communications
 - 3.2.1.2 Non-IP Wireless Communication
 - 3.2.1.3 Wireless and Wired Broadcast Communication Request
 - 3.2.1.4 Wireless Communication Testing
 - 3.2.2 Non-IP Control Networks
 - 3.2.3 IP Control Networks
 - 3.2.3.1 IP Network Routers
 - 3.2.3.2 IP Devices With Multiple Ethernet Connections
 - 3.2.4 Cryptographic Protection
 - 3.2.5 Device Identification and Authentication
 - 3.2.5.1 For Lighting Control System Devices
 - 3.2.6 Cryptographic Module Authentication
- 3.3 ACCESS CONTROL REQUIREMENTS
 - 3.3.1 User Accounts
 - 3.3.1.1 Computers
 - 3.3.1.2 Controllers
 - 3.3.1.2.1 Lighting Control Systems
 - 3.3.2 Unsuccessful Logon Attempts
 - 3.3.2.1 Devices MINIMALLY Supporting Accounts
 - 3.3.2.2 Devices FULLY Supporting Accounts
 - 3.3.3 System Use Notification
 - 3.3.3.1 System Use Notification for Remote User Interfaces
 - 3.3.3.2 System Use Notification for Local User Interfaces
 - 3.3.4 Permitted Actions Without Identification or Authentication
 - 3.3.5 Enclosures
- 3.4 USER IDENTIFICATION AND AUTHENTICATION
 - 3.4.1 User Identification and Authentication for All System Types

- 3.4.2 User Identification and Authentication for Specific System Types
 - 3.4.2.1 Lighting Control Systems Devices
- 3.4.3 Implementation of Identification and Authorization Requirements
- 3.4.4 Password-Based Authentication Requirements
 - 3.4.4.1 Passwords for Software and Applications Running on Computers
 - 3.4.4.2 Passwords for Controllers FULLY Supporting Accounts
 - 3.4.4.3 Passwords for Remote Interfaces
 - 3.4.4.4 Passwords for Devices Minimally Supporting Accounts
 - 3.4.4.5 Password Configuration and Reporting
- 3.4.5 Authenticator Feedback
- 3.5 CYBERSECURITY AUDITING
 - 3.5.1 Audit Events, Content of Audit Records, and Audit Generation
 - 3.5.1.1 Computers
 - 3.5.1.1.1 Audited Events
 - 3.5.1.1.2 Audit Event Information To Record
 - 3.5.1.2 For Lighting Control System Controller
 - 3.5.1.2.1 Lighting Control System Controllers FULLY Supporting User Accounts
 - 3.5.1.2.1.1 Audited Events
 - 3.5.1.2.1.2 Audit Event Information To Record
 - 3.5.1.2.2 Other Lighting Control System Controllers
 - 3.5.2 Audit Time Stamps
 - 3.5.3 Auditing Front End Software
 - 3.5.3.1 Import and Upload Requirements
 - 3.5.3.2 Export Requirements
 - 3.5.4 Audit Storage Capacity and Audit Upload
 - 3.5.4.1 Device Audit Record Upload Software
 - 3.5.5 Response to Audit Processing Failures
- 3.6 REQUIREMENTS FOR LEAST FUNCTIONALITY
 - 3.6.1 Device Capabilities
 - 3.6.2 Software
- 3.7 SYSTEM AND COMMUNICATION PROTECTION
 - 3.7.1 Collaborative Computing
 - 3.7.2 Denial of Service Protection
- 3.8 SAFE MODE AND FAIL SAFE OPERATION
- 3.9 SYSTEM MAINTENANCE TOOL SOFTWARE
- 3.10 VULNERABILITY SCANNING
 - 3.10.1 Computers and Software Running on Computers
 - 3.10.2 Controllers
- 3.11 FIPS 201-2 REQUIREMENT
- 3.12 SYSTEM AND INTEGRATION INTEGRITY
 - 3.12.1 Malicious Code Protection
- 3.13 CONTROL SYSTEM CYBERSECURITY TESTING
 - 3.13.1 Control System Cybersecurity Testing Procedures
 - 3.13.2 Control System Cybersecurity Testing Execution
 - 3.13.3 Control System Cybersecurity Testing Report
- AM0003* 3.14 FIELD QUALITY CONTROL, CYBERSECURITY VALIDATION SUPPORT *AM0003
- 3.15 CYBERSECURITY TRAINING

-- End of Section Table of Contents --

SECTION 25 05 11.04

CYBERSECURITY FOR FACILITY-RELATED CONTROL SYSTEMS: LIGHTING CONTROL SYSTEM

PART 1 GENERAL

Many subparts in this Section contain text in curly braces ("{" and "}") indicating which cybersecurity control and control correlation identifier (CCI) the requirements of the subpart relate to. The text inside these curly braces is for Government reference only and enables coordination of the requirements of this Section with the RMF process throughout the design and construction process. Text in curly braces are not contractor requirements.

This Section refers to Security Requirements Guide (SRGs) and Security Technical Implementation Guide (STIGs). STIGs and SRGs are available online at the Information Assurance Support Environment (IASE) website at <https://public.cyber.mil/stigs/downloads/> and an SRG/STIG Applicability Guide and Collection Tool is available at <https://public.cyber.mil/stigs/SCAP/>. Not all control system components have applicable STIGs or SRGs. The "Control Systems SRG" does not apply to work performed under this Section; all requirements within this section to apply applicable SRGs DO NOT include the "Control Systems SRG".

1.1 CONTROL SYSTEM APPLICABILITY

There are multiple versions of this Section associated with this project. Different versions have requirements applicable to different control systems. This specific Section applies only to the following control systems: LCS.

1.2 RELATED REQUIREMENTS

This section does not contain sufficient requirements to procure a control system and must be used in conjunction with other Sections which specify control systems. This Section adds cybersecurity requirements to the control systems specified in other Sections, and as these requirements are conditioned on the control system being provided, there may be requirements in this Section that will not apply to this project. All Sections containing facility-related control systems or control system components are related to the requirements of this Section. Review all specification sections to determine related requirements.

In cases where a requirement is specified in both this Section and in another Section, the more stringent requirement must be met. In cases where a requirement in this Section conflicts with the requirements of another Section such that both requirements cannot be met at the same time, request direction from the Contracting Officer to determine which requirement applies to the project.

1.3 REFERENCES

The publications listed below form a part of this specification to the extent referenced. The publications are referred to within the text by the basic designation only.

AMERICAN SOCIETY OF HEATING, REFRIGERATING AND AIR-CONDITIONING
ENGINEERS (ASHRAE)

ASHRAE 135

(2020; Interpretation 1-8 2021; Errata 1-2 2021; Addenda CD 2021; Addenda BV-CE 2022; Interpretation 9-12 2022; Interpretation 13-24 2023; Addenda BV-CF 2023; Errata 3 2023) BACnet—A Data Communication Protocol for Building Automation and Control Networks

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS (IEEE)

IEEE 802.1x (2010) Local and Metropolitan Area Networks - Port Based Network Access Control

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

NIST FIPS 140-2 (2001) Security Requirements for Cryptographic Modules

NIST FIPS 201-2 (2013) Personal Identity Verification (PIV) of Federal Employees and Contractors

U.S. DEPARTMENT OF DEFENSE (DOD)

DODI 8551.01 (2014) Ports, Protocols, and Services Management (PPSM)

DTM 08-060 (2008) Policy on Use of Department of Defense (DoD) Information Systems - Standard Consent Banner and User Agreement

1.4 DEFINITIONS

1.4.1 Administrator Account

An administrator account is an account with full permissions to a device, application, or operating system, including the ability to create and modify other user accounts.

Note that the operating system Administrator Account may be different than Administrator Accounts for applications hosted on that operating system. Also, most controllers will not have any support for accounts and will therefore not have an 'Administrator Account'.

1.4.2 Computer

A computer is one of the following:

- a. a device running a non-embedded desktop or server version of Microsoft Windows
- b. a device running a non-embedded version of MacOS
- c. a device running a non-embedded version of Linux
- d. a device running a version or derivative of the Android Operating System, where Android is considered separate from Linux
- e. a device running a version of Apple iOS

Unless otherwise indicated or clear from context use of the word "device" in this Section includes computers.

1.4.3 Controller

A device other than a computer or Ethernet switch.

1.4.4 Mission Space

A device or media is in mission space if physical access to the device or media is controlled by the organization served by the device. For example, a variable air volume (VAV) box controller in a suspended ceiling is in mission space if the VAV box serves that room; an electrical switchgear in an

electrical room or an air handling unit (AHU) in a mechanical room or on a rooftop may still be considered to be in mission space if the organization (mission) served by that switchgear or AHU controls access to the electrical room, mechanical room or rooftop.

1.4.5 Network

A network is a group of two or more devices that can communicate using a network protocol. Network protocols must provide a method for addressing devices on the network; a communication method that does not provide an addressing scheme is not a networked form of communication. Devices that communicate using a method of communication that does not support device addressing are not using a network. Addresses may be other than IP addresses, and addressing may be at either Open Systems Interconnection (OSI) layer 2 or layer 3.

1.4.6 Network Connected

A component is network connected (or "connected to a network") only when the device has a network transceiver which is directly connected to the network and implements the network protocol. A device lacking a network transceiver (and accompanying protocol implementation) can never be considered network connected. Note that (unlike many IT definitions of "Network Connected") a device connected to a non-IP network is still considered network connected (an IP connection or IP address is not required for a device to be network connected).

1.4.6.1 Wireless Network Connected

Any device that supports wireless network communication is network connected to a wireless network, regardless of whether the device is communicating using wireless. Unless physically disabled, devices with wireless transceivers support wireless, it is not sufficient to disable the wireless in software.

1.4.7 Network Media

The thing that provides the communication channel between the devices on a network. Typically wire, but might include wireless, fiber optic, or even power line (some network protocols allow sending network signals over power wiring).

1.4.8 User Account Support Levels

The support for user accounts is categorized in this Section as one of three levels:

1.4.8.1 FULLY Supported

Device supports configurable individual accounts. Accounts can be created, deleted, modified, etc. Privileges can be assigned to accounts. These devices support user-based (as opposed to role-based) authentication.

1.4.8.2 MINIMALLY Supported

Device supports a small, fixed number of accounts (perhaps only one). Accounts cannot be modified. A device with only a "User" and an "Administrator" account would fit this category. Similarly, a device with two PINs for logon - one for restricted and one for unrestricted rights would fit here (in other words, the accounts do not have to be the traditional "username and password" structure). These devices typically only support role-based authentication.

Examples of devices which MINIMALLY support accounts are a) a variable frequency drive with a single account which requires a PIN for access to configuration; and b) a room lighting control touchpad interface that has a single account.

1.4.8.3 NOT Supported

Device does not support any Access Enforcement therefore the whole concept of "account" is

meaningless.

1.4.9 Manual Local Input

Manual Local Inputs are system analog or binary inputs that are adjustable by a person but are, by intrinsic hardware design, very limited in potential capabilities. Manual Local Inputs do not have touch screens or full keyboards, but may have a few buttons or dials to allow input. Manual Local Inputs do not have full graphic screens or dot-matrix displays, but may have simple lights (LEDs) or 7-segment displays. Manual Local Inputs do not have any sort of menu structure, each button has a single well-defined function.

Examples of Manual Local Inputs are H-O-A switches, simple thermostats, and disconnect switches.

1.4.10 Card Reader

A card reader is an input/output device whose primary function is to assist in two-factor authentication. A card reader must have an interface to read data from a card and may be able to write data to a card. A card reader may have a means (such as buttons, keypad, touchscreen, etc.) for a user to input a PIN or password, as well as a limited display.

1.4.11 User Interface

A User Interface (UI) is something other than a Manual Local Input or Card Reader that allows a person to interact with the system or device. Note that while a Card Reader is not by itself a User Interface, a User Interface may contain a Card Reader in order for it to authenticate its user. Within control systems, there are a wide range of User Interfaces.

Two important distinctions are 1) whether the user interface is Local or Remote, and 2) the effective capabilities of the User Interface to alter data, which is the "privilege" of the user interface (where effective privilege available to a specific user at a specific user interface is the combination of the greatest privilege offered by the user interface and the specific account the user is logged into).

1.4.11.1 Local User Interface

A Local User Interface is a user interface where the physical hardware the user interacts with (keyboard, buttons, display, etc.) is physically part of the device being affected. All of the relevant characteristics of the user interface are embodied within a single device.

Note that a Local UI may be able to access data in a different device, Local versus Remote in this context refers to the user interface itself; the capability to access data in a different device is covered under "Full User Interface".

1.4.11.2 Remote User Interface

A Remote User Interface implements a Client/Server model where the physical hardware the user interacts with (Client) is physically distinct from the device being affected (Server). Most or all of the security and functionality characteristics of the user interface are defined by the Server, not the Client. The Client and Server communicate via a network connection. A common example of a remote user interface is a web-based interface where the browser (client) is generally on different hardware than the web server (server). A Remote UI remains a Remote UI even if the user happens to be at a Client on the same hardware as the Server. What is important is that a) the Client may be on different hardware than the Server and b) the majority of the security and functional characteristics of the interface are defined at the Server.

Note that this definition of "remote" is consistent with that generally used in the control industry but is not aligned with the NIST 800-53 definition of "Remote", which refers to "outside the system". The term "Remote" here better aligns with the NIST 800-53 definition of "Network" (remote from within the system) Access.

1.4.11.3 Types of User Interface (by capability)

User interfaces are also categorized by their capabilities as being Read Only, Limited, or Full.

1.4.11.3.1 Read-Only User Interface

A Read Only User Interface (also referred to as a View-Only User Interface) is a user interface that only allows for reading data, it does not allow (have the capability to) modify data. A Read Only User Interface may be either Local or Remote. A User Interface that is configured to be Read Only (by some other means than the interface itself, such as using configuration software on a laptop) is a Read-Only Interface. Note a Read Only User Interface may have buttons (or touch screen, etc.) allowing the user to navigate through the presentation of data.

Examples of a Read Only User Interfaces are a) a publicly viewable "energy dashboard" showing weather data and energy usage within a building and b) digital wayfinding signage.

1.4.11.3.2 Limited User Interface

A Limited User Interface is a user interface that - by design - can only alter information local to the user interface. Note that the determination of "alter" includes only direct interactions, it explicitly excludes interactions that might occur as secondary effects. For example, an interface changing the flow setpoint in a pump controller is a direct interaction, the subsequent change in flow (as well as any subsequent downstream changes in valve position) are not direct interactions.

Two examples of LIMITED UIs are: a) a variable speed drive has a Limited Local User Interface which allows the user to change properties within the drive, but does not allow affecting things outside the drive; and b) a typical home WiFi Router has a Limited Remote User Interface which allows configuration of the Router, but does not allow direct interaction with other devices.

1.4.11.3.3 Full User Interface

A Full User Interface can alter information in devices outside the device with the user interface. For example, a typical Local Display Panel is a Full Local User Interface while a browser-based front end is a Full Remote User Interface.

1.4.11.3.4 View-Only User Interface

See Read-Only User Interface

1.4.11.4 Other User Interface Terminology

In addition to defining whether a user interface is a Hardware Limited, Read-Only, Limited or Full, and whether it is Local or Remote, user interfaces are classified by whether they are writable or privileged.

1.4.11.4.1 Writable User Interface

Any User Interface that is not Read-Only is Writable. (Limited User Interfaces and Full User Interfaces are both writable user interfaces (as they are capable of changing a value)).

1.4.11.4.2 Privileged User Interface

A Privileged UI is a UI that has sufficient capabilities or functionality that it requires specific cybersecurity measures to be put in place to limit its unauthorized use. Ultimately, whether a specific user interface is considered a Privileged User Interface must be determined by usage. Unless otherwise specified, user interfaces can be determined to be privileged or not using the following:

- a. Read-Only User Interfaces are not privileged user interfaces.
- b. Full User Interfaces are privileged user interfaces.

- c. User interfaces that allow for configuration of auditing or allows for modification or deletion of audit logs are privileged user interface.
- d. User interfaces that allow for reprogramming a network connected device is a privileged user interface.
- e. Except as specified above, a Limited User Interface must be determined to be privileged or not based on the specific capabilities and use case of the user interface. In general however, user interfaces that do not offer significant capabilities above and beyond those available at that location via other means (e.g. such as a disconnect switch, breaker, or hand-off-auto switch, or physical attack) are not privileged.

1.4.12 Wireless Network

Any network that communicates without using wires or fiber optics as the communication media. Wireless networks include: WiFi, Bluetooth, ZigBee, cellular, satellite, long and short wave radio, 2.4 GHz, free space optical, point-to-point laser, microwave, and IR.

1.4.13 Wired Broadcast Network

Wired Broadcast Networks are any network, such as powerline carrier networks and modem (wired telephony), that use wire-based technologies where there is not a clearly defined boundary for signal propagation.

1.5 ADMINISTRATIVE REQUIREMENTS

1.5.1 Points of Contact

Coordinate with the following Points of Contact as indicated in this Section and as required. Not all projects will require coordination with all Points of Contact. When coordination is required and no Point of Contact is indicated, coordinate with the Contracting Officer (KO).

- a. Government Computer Access Point of Contact: Contracting Office (KO)
- b. HTTPS Certificate Point of Contact: Contracting Officer (KO)
- c. Email Address Point of Contact: Contracting Officer (KO)
- d. Password Point of Contact: Contracting Officer (KO)
- e. Mobile Code Point of Contact: Contracting Officer (KO)
- f. PKI Infrastructure Point of Contact: Contracting Officer (KO)

1.5.2 Coordination

Coordinate the execution of this Section with the execution of all other Sections related to control systems as indicated in the paragraph RELATED REQUIREMENTS. Items that must be considered when coordinating project efforts include but are not limited to:

- a. If requesting permission for wireless or wired broadcast communication, the Wireless and Wired Broadcast Communication Request submittal must be approved prior to control system device selection and installation.
- b. If requesting permission for alternate account lock permissions, the Device Account Lock Exception Request must be approved prior to control system device selection and installation.
- c. If requesting permission for the use of a device with multiple physical connections to IP networks,

the Multiple IP Connection Device Request must be approved prior to control system device selection and installation.

- d. Wireless testing may be required as part of the control system testing. See requirements for the Wireless Communication Test Report submittal.
- e. If the Device Audit Record Upload Software is to be installed on a computer not being provided as part of the control system, coordination is required to identify the computer on which to install the software.
- f. The Cybersecurity Interconnection Schedule must be coordinated with other work that will be interconnected to, and interconnections must be approved by the Government before relying on them for system functionality.
- g. Cybersecurity testing support must be coordinated across control systems and with the Government cybersecurity testing schedule.
- h. Passwords must be coordinated with the indicated contact for the project site.
- i. If applicable, HTTPS web server certificates must be obtained from the indicated HTTPS Certificate Point of Contact.
- j. Contractor Computer Cybersecurity Compliance Statements must be provided for each contractor using contractor owned computers.

1.6 SUBMITTALS

Government approval is required for submittals with a "G" or "S" classification. [Submittals not having a "G" or "S" classification are for information only. When used, a code following the "G" classification identifies the office that will review the submittal for the Government.](#) Submit the following in accordance with Section [01 33 00 SUBMITTAL PROCEDURES](#):

SD-01 Preconstruction Submittals

Wireless and Wired Broadcast Communication Request; G

Device Account Lock Exception Request; G

Multiple Ethernet Connection Device Request; G

Contractor Computer Cybersecurity Compliance Statements; G

Contractor Temporary Network Cybersecurity Compliance Statements; G

Cybersecurity Interconnection Schedule ; G

Proposed STIG and SRG Applicability Report; G

Pre-Construction Control System Inventory Report ; G

SD-02 Shop Drawings

Network Communication, Ports, Protocols and Services Report; G

Cybersecurity Network (Riser) Diagram ; G

SD-03 Product Data

Control System Cybersecurity Documentation; G

SD-06 Test Reports

Wireless Communication Test Report; G
Control System Cybersecurity Testing Procedures; G
Control System Cybersecurity Testing Report; G

SD-07 Certificates

Software Licenses; G

SD-11 Closeout Submittals

Confidential Password Report; G
Enclosure Keys; G
Software and Configuration Backups; G
Auditing Front End Software; G
Device Audit Record Upload Software; G
System Maintenance Tool Software; G
Control System Scanning Tools; G
STIG, SRG and Vendor Guide Compliance Result Report; G
Final Control System Inventory Report; G

1.7 CYBERSECURITY DOCUMENTATION

{For Government Reference Only: This subpart (and its subparts) relates to PL-7; CCI-003071}

1.7.1 Proposed STIG and SRG Applicability Report

For each model of network connected or network infrastructure device, use the DISA SRG/STIG Applicability Guide and Collection Tool (available at <https://public.cyber.mil/stigs/SCAP/>) to identify applicable STIGs or SRGs and provide a report indicating applicable STIGs and SRGs for each model. Provide the Proposed STIG and SRG Applicability Report concurrently with the Pre-Construction Control System Inventory Report.

1.7.2 Cybersecurity Interconnection Schedule

{For Government Reference Only: This subpart relates to CA-3(b), PL-8, SC-7(9), SC-7(11); CCI-000258, CCI-003072, CCI-003073, CCI-003075, CCI-002398, CCI-002399, CCI-002401, CCI-002402, CCI-002403.}

Provide a completed Cybersecurity Interconnection Schedule documenting network connections between the installed system and other systems. Provide the following information for each device directly communicating between systems: Device Identifier, Device Manufacturer, Device Description, Transport layer Protocol, Network Address, Port (if applicable), MAC (Layer 2) address (if applicable), Media, Application Protocol, Service (if applicable), Descriptive Purpose of communication. If other control system Sections used on this project include submittals documenting this information, provide copies of those submittals to meet this requirement.

In addition to the requirements of Section 01 33 00 SUBMITTAL PROCEDURES, provide the Cybersecurity Interconnection Schedule as an editable Microsoft Excel file (a template Cybersecurity Interconnection Schedule in Excel format is available at <https://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-25-05-11>.)

1.7.3 Network Communication, Ports, Protocols and Services Report

{For Government Reference Only: This subpart (and its subparts) relates to CA-9, PL-8; CCI-002102, CCI-002103, CCI-002104, CCI-002105, CCI-003072, CCI-003073, CCI-003075 and also the submittal requirements associated with CM-6, CM-7, including CM-7(3), CCI-000388.}

Provide a Network Communication, Ports, Protocols and Services Report. For each networked device, document device identifier and the communication characteristics of the device including communication protocols, services used, encryption employed, and a general description of what information is communicated over the network. For each device using IP communication, document all TCP and UDP ports used. For each device using non-IP communication, document communication protocol and media used. If other control system Sections used on this project include submittals documenting this information, provide copies of those submittals to meet this requirement.

In addition to the requirements of Section 01 33 00 SUBMITTAL PROCEDURES, provide the Network Communication, Ports, Protocols and Services Report as an editable Microsoft Excel file.

1.7.4 Control System Inventory Reports

{For Government Reference Only: This subpart (and its subparts) relates to CM-8(a), SI-17, IA-3; CCI-000389, CCI-000392, CCI-000398, CCI-002773, CCI-002774, CCI-002775, CCI-000777, CCI-000778, CCI-001958}

Provide a [Pre-Construction Control System Inventory Report](#) report and a [Final Control System Inventory Report](#), using the Inventory Spreadsheet listed under this Section at <https://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-25-05-11>. In the Control System Inventory Reports, document all devices, including networked devices, network infrastructure devices, non-networked devices, input devices (e.g. sensors) and output devices (e.g. actuators). For each device provide all applicable information for which there is a field on the spreadsheet in accordance with the instructions on the spreadsheet.

In addition to the requirements of Section 01 33 00 SUBMITTAL PROCEDURES, provide the Control System Inventory Reports as editable Microsoft Excel files. Provide the Pre-Construction Control System Inventory Report concurrently with the Proposed STIG and SRG Applicability Report

1.7.5 Software and Configuration Backups

{For Government Reference Only: This subpart (and its subparts) relates to CP-10; CCI-000550, CCI-000551, CCI-000552}

For each computer on which software is installed under this project, provide a recovery image of the final as-built computer. This image must allow for bare-metal restore such that restoration of the image is sufficient to restore system operation to the imaged state without the need for re-installation of software. If additional user permissions are required to meet this requirement, coordinate the creation of the image with the identified Government Computer Access Point of Contact.

For all Ethernet switches provide a backup of the switch configuration. For all controllers, provide a backup of the controller configuration and the source code for all loaded application programs (all software that is not common to every controller of the same manufacturer and model).

If any or all of these are provided under another Section, provide documentation indicating this and referencing those submittals.

1.7.6 Cybersecurity Network (Riser) Diagram

{For Government Reference Only: This subpart (and its subparts) relates to PL-2(a), PL-8; CCI-003051, CCI-003053, CCI-003072, CCI-003073, CCI-003075}

Provide a cybersecurity network (riser) diagram of the complete control system including all network and device hardware. For each device, include the device identifier, device type, and manufacturer. If the control system specifications require a riser diagram submittal, provide a copy of that submittal as the cybersecurity riser diagram. Otherwise, provide a riser diagram in one-line format.

1.7.7 STIG, SRG and Vendor Guide Compliance Result Report

For every component (device or software) with an applicable STIG or SRG in the Proposed STIG and SRG Applicability Report, document compliance with the STIG or SRG requirements.

- a. For components which are scannable by the Evaluate-STIG tool (available online at [\(CAC Required\)](#)), include the Evaluate-STIG report and raw scan results in addition to the final, manually reviewed and revised, documentation of compliance with STIG and SRG requirements. Checklist files should not contain any findings with a Not Reviewed (NR) status after manual reviews.
- b. For components which do not support automated scanning, a manual review using the General Purpose STIG option should be done. A completed Checklist file should not contain any findings with a Not Reviewed (NR) status after manual reviews

For every component (device or software) with manufacturer provided cybersecurity documentation, procedure, or method for secure configuration or installation, provide a report documenting how the component was configured and any deviation from the manufacturer instructions.

1.7.8 Control System Cybersecurity Documentation

{For Government Reference Only: This subpart (and its subparts) relates to SA-5(a),SA-5(b),SA-5(c), SA-22(b); CCI-003124, CCI-003125, CCI-003126, CCI-003127, CCI-003128, CCI-003129, CCI-003130, CCI-003131, CCI-003374}

Provide a Control System Cybersecurity Documentation submittal containing the indicated information for each device and software application.

1.7.8.1 Software Applications

For all software applications running on computers provide:

- a. administrator documentation that describes secure configuration of the software {For Government Reference Only: relates to CCI-003124}
- b. administrator documentation that describes secure installation of the software and software updates. {For Government Reference Only: relates to CCI-003125}
- c. administrator documentation that describes secure operation of the software {For Government Reference Only: relates to CCI-003124}
- d. administrator documentation that describes effective use and maintenance of security functions or mechanisms for the software {For Government Reference Only: relates to CCI-003127}
- e. administrator documentation that describes known vulnerabilities regarding configuration and use of administrative (i.e. privileged) functions for the software {For Government Reference Only: relates to CCI-003128}

- f. user documentation that describes user-accessible security functions or mechanisms in the software and how to effectively use those security functions or mechanisms {For Government Reference Only: relates to CCI-003129}
- g. user documentation that describes methods for user interaction which enables individuals to use the software in a more secure manner {For Government Reference Only: relates to CCI-003130}
- h. user documentation that describes user responsibilities in maintaining the security of the software {For Government Reference Only: relates to CCI-003131}

1.7.8.2 For Lighting Control System Devices

1.7.8.2.1 Lighting Control System Devices FULLY Supporting User Accounts

For all Lighting Control System Devices which FULLY support user accounts, provide:

- a. Documentation that describes secure configuration of the device {For Government Reference Only: relates to CCI-003124}
- b. Documentation that describes secure operation of the device {For Government Reference Only: relates to CCI-003124}
- c. Documentation that describes effective use and maintenance of security functions or mechanisms for the device {For Government Reference Only: relates to CCI-003127}
- d. Documentation that describes known vulnerabilities regarding configuration and use of administrative (i.e. privileged) functions for the device {For Government Reference Only: relates to CCI-003128}
- e. Documentation that describes user-accessible security functions or mechanisms in the device and how to effectively use those security functions or mechanisms; or a specific indication that there are no user-accessible security functions or mechanisms in the device {For Government Reference Only: relates to CCI-003129}
- f. Documentation that describes methods for user interaction which enables individuals to use the device in a more secure manner {For Government Reference Only: relates to CCI-003130}

1.7.8.2.2 All Other Lighting Control System Devices

For all Lighting Control System Devices which do not FULLY support user accounts, provide:

- a. Documentation that describes secure configuration of the device; or a specific indication that there are no secure configuration steps that apply {For Government Reference Only: relates to CCI-003124}
- b. Documentation that describes effective use and maintenance of security functions or mechanisms for the device; or a specific indication that there are no security functions or mechanisms in the device {For Government Reference Only: relates to CCI-003127}
- c. For devices which include a user interface, documentation that describes methods for user interaction which enables individuals to use the device in a more secure manner {For Government Reference Only: relates to CCI-003130}

1.8 SOFTWARE LICENSING

{For Government Reference Only: This subpart (and its subparts) relates to SI-2(a), SI-2(c), SI-7(14); CCI-001227, CCI-002605, CCI-002737}

For all software provided that has not already been licensed to the government or project site, provide a license to the project site for a period of no less than 5 years, and the license must also include the following software updates:

- a. Security and bug-fix patches issued by the software manufacturer.
- b. Security patches to address any vulnerability identified in the National Vulnerability Database at <http://nvd.nist.gov> with a Common Vulnerability Scoring System (CVSS) severity rating of MEDIUM or higher.

Provide a single [Software Licenses](#) submittal with documentation of the software licenses for all software provided

1.9 CYBERSECURITY DURING CONSTRUCTION

{For Government Reference Only: This subpart (and its subparts) relates to AC-18, CA-3; CCI-000258}

In addition to the control system cybersecurity requirements indicated in this section, meet following requirement throughout the construction process.

1.9.1 Contractor Computer Equipment

Contractor owned computers may be used for construction. Contractor computers connected to the control system, control system network, or a control system component at any point during construction must meet the following requirements:

1.9.1.1 Operating System

The operating system must be an operating system currently supported by the manufacturer of the operating system. The operating system must be current on security patches and operating system manufacturer required updates.

1.9.1.2 Anti-Malware Software

The computer must run anti-malware software from a reputable software manufacturer. Anti-malware software must be a version currently supported by the software manufacturer, must be current on all patches and updates, and must use the latest definitions file. Computers used on this project must perform a full antivirus scan at least once per day. Computers which have connected to any other network since the last full antivirus scan must perform a full antivirus scan prior to connection to the control system network or to the temporary contractor-installed IP network. Perform an antivirus scan on all removable media (e.g., external hard drives, CDs, DVDs, USB flash drives) prior to connecting to the control system environment.

1.9.1.3 Passwords and Passphrases

The passwords and passphrases for computers, applications, and web-based applications supporting passwords must be changed from their default values. Passwords must be a minimum of eight characters with a minimum of one uppercase letter, one lowercase letter, one number and one special character.

1.9.1.4 User-Based Authentication

Each user must have a unique account; sharing of a single account between multiple users is prohibited.

1.9.1.5 Demonstration of Compliance

The Government has the right to require demonstration of computer compliance with these

requirements at any time during the project.

1.9.1.6 Contractor Computer Cybersecurity Compliance Statements

Provide a single submittal containing completed Contractor Computer Cybersecurity Compliance Statements for each company using contractor owned computers. Contractor Computer Cybersecurity Compliance Statements must use the template published at <https://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-25-05-11>. Each Statement must be signed by a cybersecurity representative for the relevant company.

1.9.2 Temporary IP Networks

Temporary contractor-installed IP networks may be used during construction. When used, temporary contractor-installed IP networks connected to the control system, control system network, or a control system component at any point during construction must meet the following requirements:

1.9.2.1 Network Boundaries and Connections

The network must not extend outside the project site and must not connect to any IP network other than those specifically provided or furnished for this project. Any and all access to the network from outside the project site is prohibited.

1.9.3 Government Access to Network

Government personnel must be allowed to have complete and immediate access to the network at any time in order to verify compliance with this specification.

1.9.4 Passwords and Passphrases

The passwords and passphrases for all network devices and network access must be changed from their default values. Passwords must be a minimum 8 characters with a minimum of one uppercase letter, one lowercase letter, one number and one special character.

1.9.5 Contractor Temporary Network Cybersecurity Compliance Statements

Provide a single submittal containing completed Contractor Temporary Network Cybersecurity Compliance Statements for each company implementing a temporary IP network. Contractor Temporary Network Cybersecurity Compliance Statements must use the template published at <https://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-25-05-11>. Each Statement must be signed by a cybersecurity representative for the relevant company. If no temporary IP networks will be used, provide a single copy of the Statement indicating this.

1.10 CYBERSECURITY DURING WARRANTY PERIOD

All work performed on the control system after acceptance must be performed using Government Furnished Equipment or equipment specifically and individually approved by the Government.

PART 2 PRODUCTS

All products used on this project must meet the indicated requirements, but not all products specified here will be required by every project.

2.1 ETHERNET SWITCH

Provide Open Systems Interconnection (OSI) Layer 2 Ethernet switches with the following capabilities, and with an interface to support switch configuration for these capabilities:

2.1.1 Required Functionality

Switches must:

- a. Copper Ethernet ports must auto negotiate for 10, 100 and 1000 megabits-per-second links.
- b. Be capable of implementing port level access control by MAC address and limit the number of MAC addresses to one MAC address per port.
- c. For LOW Impact Systems, be capable of implementing per-port access control lists (ACLs) where the list can be filtered by source and destination IP addresses, and by source and destination UDP or TCP ports.

2.1.2 Configuration Requirements

Switches must:

- a. Support configuration save and restore.
- b. Support both manual IP address assignment and acquisition of a dynamic IP address via Dynamic Host Configuration Protocol (DHCP).
- c. Be capable of limiting access for configuration to one or more of: a web interface using HTTPS, a command line interface using SSH, or an SNMP connection using SNMP version 3 or later.

2.2 DAISY CHAIN IP CONTROLLERS

Controllers used as Daisy Chain IP Controllers must be IP controllers with exactly two Ethernet network connections and basic built-in switch capabilities to allow implementation of an Ethernet network in a daisy chain architecture. Switches incorporated by Daisy Chain IP Controllers are not required to meet the requirements for Ethernet Switches as defined in this Section.

PART 3 EXECUTION

3.1 CYBERSECURITY HARDENING AND CONFIGURATION GUIDES

Install, configure, and harden all hardware and software furnished on this project in accordance with manufacturer provided documentation, procedures, or methods for secure configuration or installation. Do not implement specific hardening actions if that action would conflict with required functionality or another requirement of this Section.

3.2 NETWORK REQUIREMENTS

3.2.1 Wireless and Wired Broadcast Communication

{For Government Reference Only: This subpart (and its subparts) relates to AC-18, AC-18(3); CCI-001438, CCI-001439, CCI-002323, CCI-001441, CCI-001449}

Unless explicitly authorized by the Government, do not use any wireless or wired broadcast communication.

3.2.1.1 Wireless and Wired Broadcast IP Communications

Unless specifically approved and installed in accordance with the project site requirements, Do not install wireless or wired broadcast IP networks, including: do not install a wireless access point; do not install or configure an ad-hoc wireless network; do not install or configure a WiFi Direct communication.

When explicitly authorized by the Government, wireless IP communication may be used to communicate with an existing wireless network.

3.2.1.2 Non-IP Wireless Communication

For LOW Impact Systems: When non-IP wireless communication is explicitly authorized by the Government, use the maximum level of encryption supported by the specific protocol employed and select signal strength and radiated power to the minimum necessary for reliable communication.

3.2.1.3 Wireless and Wired Broadcast Communication Request

Provide a report documenting the proposed use of wireless or wired broadcast communication prior to device selection using the Wireless and Wired Broadcast Communication Request Schedule at <https://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-25-05-11>. If there is no proposed use of wireless or wired broadcast communication, provide a document indicating this instead of the Request Schedule.

For each device proposed to use wireless or wired broadcast communication show: the device identifier, a description of the device, the location of the device, the device identifiers of other devices communicating with the device, the protocol used for communication, encryption type and strength. For wireless communication, also show: RF Frequency, Radiated Power in dBm (decibel with a milliwatt reference), free-space range, and the expected as-installed range.

3.2.1.4 Wireless Communication Testing

As part of Performance Verification Testing (PVT) Functional Performance Testing {FPT}, conduct testing of wireless communication for all devices indicated on the approved Wireless and Wired Broadcast Communication Request as requiring testing.

To test wireless communication, test for wireless network reception at multiple points along the wireless test boundary in the vicinity of the wireless device, and record whether a network connection can be established at each point. The wireless test boundary is the facility fence line. If wireless testing is required, provide a [Wireless Communication Test Report](#) documenting the testing points and results at each point for each wireless device.

3.2.2 Non-IP Control Networks

When control system specifications require particular communication protocols, use only those communication protocols and only as specified. Do not implement any other communication protocol.

When control system specifications do not indicate requirements for communication protocols, use only those protocols required for operation of the system as specified.

3.2.3 IP Control Networks

{For Government Reference Only: This subpart relates to CM-6(a), CM-7(a), CM-7(b), CM-7(1)(b), SC-41; CCI-001588, CCI-000381, CCI-000380, CCI-000381, CCI-000382, CCI-001761, CCI-001762, CCI-002544, CCI-002545, CCI-002546.}

IP Networks must be Ethernet networks and must use switches which are Ethernet Switches or Daisy Chain IP Controllers as defined in this Section. Do not use nonsecure functions, ports, protocols and services as defined in [DODI 8551.01](#) unless those ports, protocols and services are specifically required by the control system specifications or otherwise specifically authorized by the Government. Do not use ports, protocols and services that are not specified in the control system specifications or required for operation of the control system.

3.2.3.1 IP Network Routers

Do not install any device that performs IP routing.

3.2.3.2 IP Devices With Multiple Ethernet Connections

Except for Ethernet Switches and Daisy Chain IP Controllers, devices must not have more than one Ethernet connection to IP networks unless doing so is required by the project specifications and the specific application is approved. If a device with Multiple Ethernet Connections to IP networks is required, provide a [Multiple Ethernet Connection Device Request](#) using the Multiple Ethernet Connection Device Request Template at <https://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-25-05-11> to request approval for each device. If a device with Multiple Ethernet Connections to IP networks is not required, instead provide a document stating that no approval is being requested.

3.2.4 Cryptographic Protection

{For Government Reference Only: This subpart relates to IA-2(9), IA-3(1), SC-8, SC-13, SC-23(1), SC-23(3); CCI-001942, CCI-001959, CCI-001967, CCI-002418, CCI-002449, CCI-002450, CCI-001185, CCI-001188, CCI-001664.}

All remote user interfaces must use HTTPS for all traffic between the user interface client and user interface server.

For devices that have STIG/SRGs related to cryptographic protection (CCI-002450), comply with the requirements of those STIG/SRGs. Ensure that all network traffic is encrypted using NSA-approved cryptography; provision of digital signatures and hashing, and FIPS-validated cryptography.

3.2.5 Device Identification and Authentication

{For Government Reference Only: This subpart (and its subparts) relates to IA-3; CCI-000777, CCI-000778, CCI-001958.}

All computers must support and implement [IEEE 802.1x](#) for device authentication to the network.

3.2.5.1 For Lighting Control System Devices

Devices using HTTP as a control protocol must use HTTPS instead. Devices using Fox Protocol must support [IEEE 802.1x](#). Devices using Ethernet must support [IEEE 802.1x](#). Devices using BACnet must support network security as specified for BACnet Secure Connect in [ASHRAE 135](#).

3.2.6 Cryptographic Module Authentication

{For Government Reference Only: This subpart (and its subparts) relates to IA-7; CCI-000803}

For devices (including but not limited to [NIST FIPS 140-2](#) compliant radios) that have STIG/SRGs related to cryptographic module authentication (CCI-000803), comply with the requirements of those STIG/SRGs.

3.3 ACCESS CONTROL REQUIREMENTS

3.3.1 User Accounts

{For Government Reference Only: This subpart (and its subparts) relate to AC-2(a), AC-3, AC-6(1), AC-6(10), AC-6(2), AC-6(9), CM-11(2), and IA-2; CCI-002110, CCI-000213, CCI-001558, CCI-002221, CCI-002222, CCI-002223, CCI-002235, CCI-000039, CCI-001419, CCI-002234, CCI-001812, and CCI-000764.}

Any user interface supporting user accounts (either FULLY or MINIMALLY) must limit access according to specified limitations for each account. Install and configure any device having a STIG or SRG in accordance with that STIG or SRG.

All user interfaces FULLY supporting accounts must implement user-based authentication where each

account is uniquely assigned to a specific user. User interfaces FULLY supporting accounts must implement at least three (3) levels of user account privilege including: 1) an account with read-only permissions 2) an account with full permissions including account creation and modification and 3) an account with greater permissions than read-only but without account creation and modification. Disable any unnecessary or unused accounts. Disable any "guest-level" accounts that are created on the system by default.

3.3.1.1 Computers

All computer operating systems must FULLY support user accounts and implement accounts for access. Each control system software application not supporting accounts and running on a computer must be installed such that use of the software is restricted by the computer operating system to specific users.

Applications running on computers must not require the user be logged in to a computer operating system administrator account for normal operation. It is permissible to require the computer operating system administrator account for initial application installation and configuration.

3.3.1.2 Controllers

For user interfaces provided by controllers, provide access control in accordance with the User Interface Requirements table for the applicable control system and user interface type.

- a. For table entries of "NA": NA means Not Applicable, there are no interfaces in this category.
- b. For table entries of "None Required": The user interface is not required to support user accounts.
- c. For table entries of "MINIMALLY": The user interface must at least MINIMALLY support user accounts.
- d. For table entries of "FULLY": The user interface must at FULLY support user accounts.
- e. For table entries of "KEY": The user interface must have physical security in the form of either a key lock on the interface itself or be furnished inside a lockable enclosure. Where this is required for a read only interface, the lockable enclosure must prevent viewing of data on the interface; for other interfaces, this lockable enclosure must prevent using the interface to alter data.
- f. For table entries of "Physical Security": For Local FULL interfaces, the interface must be located inside mission space. For Local Limited (not FULL) interfaces, the user interface must either a) be located within mission space or b) be protected by physical security at least as good as the control devices (and equipment controlled by the control devices) affected by the interface. For purposes of this requirement, 'affected' includes controllers with data that can be directly altered by the interface, as well as mechanical and/or electrical equipment directly controlled by those controllers, but does not include other interactions.
- g. Entries of the form "X and Y" must meet both the requirement indicated for X and the requirement indicated for Y. For example, an entry of "MINIMALLY and Physical Security" indicates the user interface must both MINIMALLY support accounts and have physical security.
- h. Entries of the form "X or Y" must meet either the requirement indicated for X or the requirement indicated for Y.

3.3.1.2.1 Lighting Control Systems

User Interface Requirements for LOW Impact Lighting Control Systems	
<u>User Interface Type</u>	<u>Access Control Requirement</u>
Local Read Only (see note 1)	None Required
Local Limited, Non-privileged	MINIMALLY
Local Limited, Privileged	Physical Security
Local Full	MINIMALLY
Remote Read Only	None Required
Remote Limited, Non-Privileged	MINIMALLY
Remote Limited, Privileged AND Remote Full (see note 2)	FULLY
Notes: 1)Local Read Only User Interfaces are always Non-Privileged 2)Remote Full User Interfaces are always Privileged	

3.3.2 Unsuccessful Logon Attempts

{For Government Reference Only: This subpart (and its subparts) relate to AC-7 (a), AC-7 (b); CCI-000043, CCI-000044, CCI-001423, CCI-002236, CCI-002237, CCI-002238}

Except for high availability user interfaces indicated as exempt, devices must meet the indicated requirements for handling unsuccessful logon attempts. If a device cannot meet these requirements, document device capabilities to protect from subsequent logon attempts and propose alternate protections in a [Device Account Lock Exception Request](#) submittal. Do not implement alternate protection measures in lieu of the indicated requirements without explicit permission from the Government. If no Device Account Lock Exceptions are requested, provide a document stating that no approval is being requested as the Device Account Lock Exception Request.

3.3.2.1 Devices MINIMALLY Supporting Accounts

For LOW Impact Systems: Devices which MINIMALLY (but not FULLY) support accounts must lock the user account after five consecutive failed login attempts.

3.3.2.2 Devices FULLY Supporting Accounts

Devices which FULLY support accounts must meet the following requirements.

- It must lock the user account when three unsuccessful logon attempts occur within a 15 minute interval.
- Once an account is locked, the account must stay locked until unlocked by an administrator. If the account being locked is the sole administrator account on the device, the account must stay locked for 1 hour and then automatically unlock.
- Once the indicated number of unsuccessful logon attempts occurs, delay further logon prompts by

5 seconds.

3.3.3 System Use Notification

{For Government Reference Only: This subpart (and its subparts) relates to AC-8; CCI-000048, CCI-002247, CCI-002243, CCI-002244, CCI-002245, CCI-002246, CCI-000050, CCI-002248}

3.3.3.1 System Use Notification for Remote User Interfaces

Remote user interfaces must display a warning banner meeting the requirements of **DTM 08-060** on screen.

3.3.3.2 System Use Notification for Local User Interfaces

Devices which are connected to a network and have a local user interface must display a warning banner meeting the requirements of **DTM 08-060** on the user interface screen if capable of doing so and must have a permanently affixed label with an approved banner from **DTM 08-060** if unable to display the warning banner on the screen. Where it is impractical (perhaps due to device size) to affix the label to the device, affix the label to the device enclosure.

Labels must be machine printed or engraved, plastic or metal, designed for permanent installation, must use a font no smaller than 14 point, and must provide a high contrast between font and background colors.

3.3.4 Permitted Actions Without Identification or Authentication

{For Government Reference Only: This subpart (and its subparts) relates to AC-14; CCI-000061, CCI-000232}

The control system must require identification and authentication before allowing any actions except read-only actions by a user acting from a user interface which MINIMALLY or FULLY supports accounts.

3.3.5 Enclosures

Prior to final acceptance of the system, lock all lockable enclosures. Submit an **Enclosure Keys** submittal with all copies of keys for all enclosures and a key inventory list documenting all keys. Label each key with the matching enclosure identifier.

3.4 USER IDENTIFICATION AND AUTHENTICATION

{For Government Reference Only: This subpart (and its subparts) relates to IA-2, IA-2(1), IA-2(12), IA-5 IA-5(b), IA-5(c), IA-5(e), IA-5(g), IA-5(1), IA-5(11); CCI-000764, CCI-000765, CCI-001953, CCI-001954, CCI-001544, CCI-001989, CCI-000182, CCI-001610, CCI-000192, CCI-000193, CCI-000194, CCI-000205, CCI-001619, CCI-001611, CCI-001612, CCI-001613, CCI-001614, CCI-000195, CCI-001615, CCI-000196, CCI-000197, CCI-000199, CCI-000198, CCI-001616, CCI-001617, CCI-000200, CCI-001618, CCI-002041, CCI-002002, CCI-002003. }

This subpart indicates requirements for specific methods of identification and authentication for users and user accounts. Where these requirements conflict apply the following order of precedence: 1) If present, Device Specific Requirements take precedence over any other requirements; and then 2) multifactor authentication requirements take precedence over password requirements.

3.4.1 User Identification and Authentication for All System Types

Unless otherwise indicated, all user interfaces supporting accounts (either FULLY or MINIMALLY) must implement Identification and Authorization via passwords.

For LOW Impact Systems: User interfaces provided by computer operating systems must implement

multifactor authentication via PIV.

3.4.2 User Identification and Authentication for Specific System Types

System specific requirements are in addition to and supersede those indicated for all system types. When no additional requirements are indicated for a specific system type the requirements for all systems still apply to that system type.

3.4.2.1 Lighting Control Systems Devices

No additional system specific requirements apply

3.4.3 Implementation of Identification and Authorization Requirements

Identification and Authorization must be met by one of the following methods:

- a. Direct implementation in the user interface.
- b. For user interfaces on a computer: inheriting the Identification and Authorization from the computer operating system, either by the operating system limiting access to specific applications by user, or by the application itself having permissions based on the user logged into the computer.
- c. For remote interfaces: an implementation shared between the remote user interface server and the remote user interface client. For example, a requirement for PIV authentication may be met on a remote user interface by a PIV reader on a web browser client which sends the authentication information via HTTPS to the remote server.

3.4.4 Password-Based Authentication Requirements

3.4.4.1 Passwords for Software and Applications Running on Computers

All software and applications running on computers supporting password-based authentication must enforce the following requirements:

- a. Minimum password length of 12 characters
- b. Password must contain at least one uppercase character.
- c. Password must contain at least one lowercase character.
- d. Password must contain at least one numeric character.
- e. Password must contain at least one special character. The list of supported special characters must include at least 4 separate characters.
- f. Password must have a minimum lifetime of 24 hours.
- g. Password must have a maximum lifetime of 60 days. When passwords expire, prompt users to change passwords. Do not lock accounts due to expired passwords.
- h. Password must differ from previous five passwords, where differ is defined as changing at least 50 percent of the characters (where location is significant, a character may be reused if it is in a different position).
- i. Passwords must be cryptographically protected during storage and transmission.

3.4.4.2 Passwords for Controllers FULLY Supporting Accounts

All controllers FULLY supporting accounts and supporting password-based authentication must enforce the following requirements:

- a. Minimum password length of 12 characters
- b. Password must contain at least one uppercase character.
- c. Password must contain at least one lowercase character.
- d. Password must contain at least one numeric character.
- e. Password must contain at least one special character. The list of supported special characters must include at least 4 separate characters.
- f. Password must have a maximum lifetime of sixty (60) days. When passwords expire, prompt users to change passwords. Do not lock accounts due to expired passwords.
- g. Password must differ from previous five passwords, where differ is defined as changing at least 50 percent of the characters.
- h. Passwords must be cryptographically protected during storage and transmission.

3.4.4.3 Passwords for Remote Interfaces

Passwords for connecting to a Remote User Interface supporting password-based authentication must enforce the following requirements:

- a. Minimum password length of 12 characters
- b. Password must contain at least one uppercase character.
- c. Password must contain at least one lowercase character.
- d. Password must contain at least one numeric character.
- e. Password must contain at least one special character. The list of supported special characters must include at least 4 separate characters.
- f. Password must have a maximum lifetime of 60 days. When passwords expire, prompt users to change passwords. Do not lock accounts due to expired passwords.
- g. Password must differ from previous five passwords, where differ is defined as changing at least 50 percent of the characters (where location is significant, a character may be reused if it is in a different position).
- h. Passwords must be cryptographically protected during storage and transmission.

3.4.4.4 Passwords for Devices Minimally Supporting Accounts

Devices MINIMALLY supporting accounts must support passwords with a minimum length of four.

3.4.4.5 Password Configuration and Reporting

For all devices with a password, change the password from the default password. Coordinate selection of passwords with the Password Point of Contact. Do not use the same password for more than one device unless specifically instructed to do so. Provide a [Confidential Password Report](#) documenting the password for each device and describing the procedure to change the password for

each device.

Do not provide the Password Summary Report in electronic format. Provide two hardcopies of the Password Summary Report, each copy in its own sealed envelope.

3.4.5 Authenticator Feedback

{For Government Reference Only: This subpart relates to IA-6; CCI-000206}

Devices must never show authentication information, including passwords, on a display. Devices that momentarily display a character as it is entered, and then obscure the character, are acceptable. For devices that have STIGs or SRGs related to obscuring of authenticator feedback (CCI-000206), comply with the requirements of those STIGS/SRGs.

3.5 CYBERSECURITY AUDITING

Where an auditing requirement exists for email notification, notify via email the application administrator and Information System Security Officer (ISSO) of the event. Coordinate with the Email Address Point of Contact for email addresses. If outgoing email is not available to the system, disable email notifications.

3.5.1 Audit Events, Content of Audit Records, and Audit Generation

{For Government Reference Only: This subpart (and its subparts) relates to AU-2(a), AU-2(c), AU-2(d), AU-3, AU-10, AU-12, AU-14(b), AU-14(1), AU-14(2), AU-14(3), CM-5(1), SC-7 (9); CCI-000123, CCI-001571, CCI-000125, CCI-001485, CCI-000130, CCI-000131, CCI-000132, CCI-001230, CCI-000133, CCI-000134, CCI-001487, CCI-000166, CCI-001899, CCI-000169, CCI-001459, CCI-000171, CCI-000172, CCI-001910, CCI-001914, CCI-001919, CCI-001464, CCI-001462, CCI-001920, CCI-001814, CCI-002400. }

For devices that have STIG/SRGs related to audit events, content of audit records or audit generation, comply with the requirements of those STIG/SRGs.

If auditing requirements can be met using existing control system alarm or event capabilities, those existing capabilities may be used to meet these requirements.

3.5.1.1 Computers

For each computer, provide the capability to select audited events and the content of audit logs. Configure computers to audit the indicated events, and to record the indicated information for each auditable event. Send logs to a syslog server that is only accessible via accounts on the system with privileged level access.

3.5.1.1.1 Audited Events

Configure each computer to audit the following events:

- a. Successful and unsuccessful attempts to access, modify, or delete privileges, security objects, security levels, or categories of information (e.g. classification levels)
- b. Successful and unsuccessful logon attempts
- c. Successful logouts
- d. Privileged activities or other system level access
- e. Concurrent logons from different workstations
- f. Successful and unsuccessful accesses to objects

- g. Program initiations
- h. Direct access to the information system
- i. Account creations, modifications, disabling, and terminations.
- j. Kernel module load, unload, and restart

3.5.1.1.2 Audit Event Information To Record

Configure each computer to record, for each auditable event, the following information (where applicable to the event):

- a. What type of event occurred
- b. When the event occurred
- c. Where the event occurred
- d. The source of the event
- e. The outcome of the event
- f. The identity of any individuals or subjects associated with the event

3.5.1.2 For Lighting Control System Controller

3.5.1.2.1 Lighting Control System Controllers FULLY Supporting User Accounts

For each controller which FULLY supports accounts, provide the capability to select audited events and the content of audit logs. Configure controllers to audit the indicated events, and to record the indicated information for each auditable event.

3.5.1.2.1.1 Audited Events

Configure each controller to audit the following events:

- a. Successful and unsuccessful logon attempts to the controller
- b. Successful logouts
- c. All account creations, modifications, disabling, and terminations.
- d. All controller shutdown and startup

3.5.1.2.1.2 Audit Event Information To Record

Configure each controller to record, for each auditable event, the following information (where applicable to the event):

- a. what type of event occurred
- b. when the event occurred
- c. the identity of any individuals or subjects associated with the event

3.5.1.2.2 Other Lighting Control System Controllers

There are no requirements to perform auditing at Lighting field controllers that do not FULLY support accounts.

3.5.2 Audit Time Stamps

{For Government Reference Only: This subpart (and its subparts) relates to AU-8; CCI-000159, CCI-001889, CCI-001890.}

Any device (computer or controller) generating audit records must have an internal clock capable of providing time with a resolution of one second. Clocks must not drift more than 10 seconds per day. Configure the system so that each device (computer or controller) generating audit records maintains accurate time to within 1 second. Note that if the control system specifications include requirement for clocks, the most stringent requirement applies.

3.5.3 Auditing Front End Software

The project site currently has the following software to support control system auditing: none. If there is no existing auditing front end software or the software is not compatible with the provided control systems, provide Auditing Front End Software with audit log import and upload, export, notification, and analysis functionality. The Auditing Front End Software may be provided as a component of the control system front end or as a separate software package, and a single package may serve multiple control systems provided under the same projects if they are sharing a cybersecurity authorization.

When the Auditing Front End Software is neither existing nor installed under the requirements of another Section, furnish the Auditing Front End Software media and license and install the software on the control system front end computer. Submit copies of Auditing Front End Software if this function is not part of the software provided with the control system to meet requirements of other Sections.

3.5.3.1 Import and Upload Requirements

Auditing Front End Software must be capable of importing audit logs from the Device Audit Record Upload Software and of uploading audit logs over the network from all control system devices supporting network upload of audit logs.

3.5.3.2 Export Requirements

Auditing Front End Software must be capable of exporting to a file format supported by Microsoft Excel.

3.5.4 Audit Storage Capacity and Audit Upload

{For Government Reference Only: This subpart (and its subparts) relates to AU-4; CCI-001848, CCI-001849}

The creation of audit records must never interfere with normal device operation. Devices must cease collection of auditing information if required to maintain normal operation.

- a. For devices that have STIG/SRGs related to audit storage capacity (CCI-001848 or CCI-001849) comply with the requirements of those STIG/SRGs.
- b. For controllers capable of generating audit records, provide 60 days worth of secure local storage, assuming 10 auditable events per day.

3.5.4.1 Device Audit Record Upload Software

For each device (computer or controller) required to audit events and for which audit logs cannot be uploaded over the network by the Auditing Front End Software, provide and license to the Government software implementing a secure mechanism of uploading audit records from the device and exporting

them to the Auditing Front End Software. Where different devices use different software, provide software of each type required to upload audit logs from all devices.

When Device Audit Record Upload Software is capable of uploading audit logs over the network, install Device Audit Record Upload Software on the same computer as the Auditing Front End Software. Submit copies of device audit record upload software if this function is not part of the software provided with the control system to meet requirements of other Sections. If there are no devices requiring this software, provide a document stating this in lieu of this submittal.

3.5.5 Response to Audit Processing Failures

{For Government Reference Only: This subpart (and its subparts) relates to AU-5; CCI-000139, CCI-000140, CCI-001490.}

In the case of a failure in the auditing system, computers associated with auditing must provide email notification. In case of an audit failure, if possible, continue to collect audit records by overwriting existing audit records.

3.6 REQUIREMENTS FOR LEAST FUNCTIONALITY

{For Government Reference Only: This subpart (and its subparts), along with the Network Communication, Ports, Protocols and Services Report submittal specified elsewhere in this section, relates to CM-6(a), CM-6(c), CM-7, CM-7(1)(b), SC-41; CCI-000363, CCI-000364, CCI-000365, CCI-001588, CCI-001755, CCI-000381, CCI-000380, CCI-000382, CCI-001761, CCI-001762, CCI-002544, CCI-002545, CCI-002546. }

For devices that have a STIG or SRG related to Requirements for Least Functionality (such as configuration settings and port and device I/O access for least functionality), install and configure the device in accordance with that STIG or SRGs.

3.6.1 Device Capabilities

For Lighting Control Systems: Do not provide devices with remote user interfaces or with full user interfaces where one was not required.

For Other Control Systems: Do not provide devices with remote user interfaces or with full user interfaces where one was not required.

3.6.2 Software

For software that has a STIG or SRG related to Requirements for Least Functionality (such as configuration settings and port access for least functionality), install and configure the software in accordance with that STIG or SRG.

Do not install software that is not specifically required to meet a contract requirement. Remove any previously installed that is not specifically required to meet a contract requirement. Do not implement functionality within software that is not specifically required to meet contract requirements.

3.7 SYSTEM AND COMMUNICATION PROTECTION

3.7.1 Collaborative Computing

{For Government Reference Only: This subpart relates to SC-15(a), SC-15(b); CCI-001150, CCI-001152.}

Without explicit approval from the project site, control systems must not use collaborative computing technologies.

3.7.2 Denial of Service Protection

{For Government Reference Only: This subpart relates to SC-5, SC-12, SC-7(a); CCI-001093, CCI-002385, CCI-002386, CCI-002430, CCI-001097. }

To the greatest extent practical, implement control logic without reliance on the network. Except when required to meet the requirements of the control system Section (where the requirement can only be met using computer hardware), do not implement control logic in computers.

3.8 SAFE MODE AND FAIL SAFE OPERATION

{For Government Reference Only: This subpart (and its subparts) relates to CP-12, SI-10(3), SI-17; CCI-002855, CCI-002856, CCI-002857, CCI-002754, CCI-002773, CCI-002774, CCI-002775}

For all control system components with an applicable STIG or SRG, configure the component in accordance with all applicable STIGs and SRGs.

3.9 SYSTEM MAINTENANCE TOOL SOFTWARE

{For Government Reference Only: This subpart (and its subparts) relates to MA-3; CCI-000865.}

Submit and license to the Government all software required to operate, maintain and modify the control system such the Government or their agents are able to perform repair, replacement, upgrades, and expansions of the system without subsequent or future dependence on the Contractor, Vendor or Manufacturer. Submit hard copies of user manuals for each software with the software submittal. Provide any hardware keys or dongles, software keys, license numbers, and other information required to enable the Government to access or change the system.

For software provided and licensed to the Government under the requirements of another Section, submit a statement indicating the Section and Submittal under which the software was provided. For software provided to meet the requirements of this Section and not provided and licensed under another Section, submit software and software user manuals on DVD or CD as a Technical Data Package and submit one hard copy of the software user manual for each piece of software.

3.10 VULNERABILITY SCANNING

{For Government Reference Only: This subpart (and its subparts) relates to RA-5 RA-5(a),RA-5(b),RA-5(c),RA-5(d); CCI-001054, CCI-001055, CCI-000156, CCI-001641, CCI-001643, CCI-001057, CCI-001058, CCI-001059. }

All IP devices must be scannable, such that the device can be scanned by industry standard IP network scanning utilities without harm to the device, application, or functionality.

3.10.1 Computers and Software Running on Computers

Computers and applications running on computers must meet relevant vulnerability scanning STIGs/SRGs and respond to approved DoD vulnerability scanning tools.

3.10.2 Controllers

Provide controllers that are scannable by standard control system discovery tools or control system browsers and return meaningful status information including the network inputs and outputs for the controller. This information must contain sufficient detail to detect vulnerabilities or exploits of the controller.

Provide all software needed to scan the control system as the [Control System Scanning Tools](#) submittal. If the software required to scan the system is already installed at the project site or is provided under a separate section instead provide a statement indicating this.

3.11 FIPS 201-2 REQUIREMENT

{For Government Reference Only: This subpart (and its subparts) relates to SA-4 (10); CCI-003116}

Devices in the following systems which implement PIV must be on the **NIST FIPS 201-2** approved product list (<https://www.idmanagement.gov/approved-products-list/>): LCS.

3.12 SYSTEM AND INTEGRATION INTEGRITY

3.12.1 Malicious Code Protection

{For Government Reference Only: This subpart (and its subparts) relates to SI-3(c); CCI-001241, CCI-002623}

For all computers installed under this project, provide malware protection software media, provide licenses, and install and configure malware protection software as indicated. Coordinate with the Government Computer Access Point of Contact as required.

- a. Provide malware protection software licenses.
- b. Provide malware protection software media.
- c. Install and configure malware protection software in accordance with the relevant STIGs.

3.13 CONTROL SYSTEM CYBERSECURITY TESTING

3.13.1 Control System Cybersecurity Testing Procedures

Prepare and submit Control System Cybersecurity Testing Procedures explaining step-by-step, the actions and expected results that will demonstrate that the control system meets the requirements of this Section. The Control System Cybersecurity Testing Procedures may be submitted as a Technical Data Package.

3.13.2 Control System Cybersecurity Testing Execution

Using the Control System Cybersecurity Testing Procedures verify that the control system meets the requirements of this Section. **UNLESS GOVERNMENT WITNESSING OF A TEST IS SPECIFICALLY WAIVED BY THE GOVERNMENT, PERFORM ALL TESTS WITH A GOVERNMENT WITNESS.** If testing reveals deficiencies in the system, correct the deficiency and retest until successful.

3.13.3 Control System Cybersecurity Testing Report

Prepare and submit a Control System Cybersecurity Testing Report documenting all tests performed and their results. Include all tests in the Control System Cybersecurity Testing Procedures and any additional tests performed during testing. Document test failures and repairs conducted with the test results. The Control System Cybersecurity Testing Report may be submitted as a Technical Data Package

3.14 FIELD QUALITY CONTROL, CYBERSECURITY VALIDATION SUPPORT

AM0003*

In addition to testing and testing support required by other Sections, provide a minimum of ~~120~~16 hours of technical support for cybersecurity testing of control systems to support the DoD Risk Management Framework process Cybersecurity assessment of the control system. This support is independent of (and in addition to) the Control System Cybersecurity Testing specified in this section.

*AM0003

3.15 CYBERSECURITY TRAINING

Provide eight hours of classroom and hands-on training for six Government personnel on the cybersecurity operation and maintenance of the control system provided. This training is in addition to and must be coordinated with control system training specified in other Sections.

The Government will provide the training location. Training must cover, at a minimum: (a) applying software and firmware updates, (b) user account creation, modification and deletion, (c) audit log upload procedures and (d) identification of privileged user interfaces and system impact of those interfaces. Training session must include a question and answer period during which government staff questions about cybersecurity aspects of the control system are answered.

-- End of Section --

SECTION TABLE OF CONTENTS

DIVISION 31 - EARTHWORK

SECTION 31 63 26

DRILLED CAISSONS

PART 1 GENERAL

- *AM0003 1.1 UNIT PRICES
 - 1.1.1 Basis of Bids AM0003*
- 1.2 REFERENCES
- 1.3 SUBMITTALS
- 1.4 QUALITY ASSURANCE
 - 1.4.1 Survey of Caisson Locations
 - 1.4.2 Specialty Subcontractor Qualifications
 - 1.4.3 Welding
 - 1.4.4 Pre-installation Conference
 - 1.4.5 Contractor Supervision
 - 1.4.6 Government Inspection
 - 1.4.7 Safety Precautions for Workmen and Inspectors
 - 1.4.7.1 Life Line
 - 1.4.7.2 Ventilation
- 1.5 DELIVERY, STORAGE, and HANDLING
- 1.6 PROJECT/SITE CONDITIONS
 - 1.6.1 Subsurface Data
 - 1.6.2 Caisson Drilling Equipment
- 1.7 SEQUENCING
 - 1.7.1 Caisson Excavation
 - 1.7.2 Acceptance

PART 2 PRODUCTS

- 2.1 MATERIALS
 - 2.1.1 Concrete Work
 - 2.1.1.1 Strength
 - 2.1.1.2 Coarse Aggregate
 - 2.1.1.3 Reinforcing Steel
 - 2.1.2 Welding
 - 2.1.3 Casing Steel
- 2.2 CAISSON DRILLING EQUIPMENT

PART 3 EXECUTION

- 3.1 PREPARATION
- 3.2 INSTALLATION
- 3.3 TOLERANCES
- 3.4 PROTECTION
- 3.5 RECORDS

-- End of Section Table of Contents --

SECTION 31 63 26
DRILLED CAISSONS

PART 1 GENERAL

*AM0003 1.1 UNIT PRICES

1.1.1 Basis of Bids

Base the bid on the number and total length of caissons, established by top and bottom elevations and diameters, as indicated and specified. Adjustment of the contract will be made, should the total length of caissons installed and approved be greater or less than the total length shown. The Contractor will not receive payment for rejected caissons or for those not conforming to specifications.

AM0003*

1.2 REFERENCES

The publications listed below form a part of this specification to the extent referenced. The publications are referred to within the text by the basic designation only.

AMERICAN WELDING SOCIETY (AWS)

AWS D1.1/D1.1M (2020; Errata 1 2021) Structural Welding Code - Steel

AWS D1.4/D1.4M (2018) Structural Welding Code - Reinforcing Steel

ASTM INTERNATIONAL (ASTM)

ASTM A36/A36M (2019) Standard Specification for Carbon Structural Steel

ASTM A123/A123M (2024) Standard Specification for Zinc (Hot-Dip Galvanized) Coatings on Iron and Steel Products

ASTM A615/A615M (2022) Standard Specification for Deformed and Plain Carbon-Steel Bars for Concrete Reinforcement

1.3 SUBMITTALS

Government approval is required for submittals with a "G" or "S" classification. Submittals not having a "G" or "S" classification are for information only. When used, a code following the "G" classification identifies the office that will review the submittal for the Government. Submit the following in accordance with Section 01 33 00 SUBMITTAL PROCEDURES:

SD-02 Shop Drawings

Caissons; G, DO

Survey of Caisson Locations; G

SD-07 Certificates

Caissons

Qualifications; G, DO

Records for Each Qualified Welding Operator; G, G

SD-11 Closeout Submittals

Records

1.4 QUALITY ASSURANCE

1.4.1 Survey of Caisson Locations

Submit a certified survey meeting the requirements specified herein.

1.4.2 Specialty Subcontractor Qualifications

Submit Contractor [Qualifications](#) for foundation systems, proving its engagement in the successful installation of similar drilled foundation caissons for at least 5 years.

1.4.3 Welding

Perform all detail and field welding in accordance with [AWS D1.1/D1.1M](#). Qualification of welding procedures, welders, and welding operators must be in accordance with [AWS D1.1/D1.1M](#), Section 4. Keep and make available, for examination by the Contracting Officer, all records of test results of welding procedures not prequalified, copies of records for each qualified welding operator, and records on positions of welding and types of electrode qualifications. Submit [records for each qualified welding operator](#).

1.4.4 Pre-installation Conference

At the Pre-installation conference provide, for approval, the following schedule of submittals: Preliminary detailed drawings in an approved form, for each caisson, showing shaft and bell diameters, depths of test holes, top and bottom elevations, bearing strata description, casing description, water conditions, concrete strength, concrete volume, rock elevations, dates of excavation and concrete placement, and other pertinent information.

1.4.5 Contractor Supervision

Provide for the supervision of all phases of drilled pier construction. Supervision is the Contractor's responsibility as outlined in Quality Control provisions of the Specialty Subcontractor Requirements. Check each drilled pier excavation for its depth, water removal, cleanup, workmanship, and for all tolerance requirements before any concrete is placed.

1.4.6 Government Inspection

The Contracting Officer will inspect each drilled pier excavation. Do not place concrete until the excavation has been approved by the Contracting Officer. Furnish the Contracting Officer all necessary equipment required for proper inspection of drilled pier excavations.

1.4.7 Safety Precautions for Workmen and Inspectors

1.4.7.1 Life Line

Provide each person, entering a drilled pier excavation, with a life line suitable for instant rescue, securely fastened to a shoulder harness, separated from any line used to remove excavated materials, and rigged so that the person can be immediately hoisted out of the excavation in an emergency. Do not lower any person into a drilled pier excavation prior to casing the shaft through the overburden.

1.4.7.2 Ventilation

Provide each drilled pier excavation with a ventilating device of sufficient capacity to ensure a safe and healthy atmosphere before workmen and inspectors are permitted to enter the drilled pier excavation

and during all work periods.

1.5 DELIVERY, STORAGE, and HANDLING

Deliver casings and appurtenant equipment to the job site in an undamaged and ready to place condition. Deliver concrete in accordance with requirements of 03 30 00 CAST-IN-PLACE CONCRETE.

1.6 PROJECT/SITE CONDITIONS

1.6.1 Subsurface Data

The subsurface investigation report and samples of materials, as taken from subsurface investigations, are available for examination at USACE Fort Worth District.

1.6.2 Caisson Drilling Equipment

Provide caisson drilling equipment having a minimum torque capacity and downward force capacity for the contract site conditions.

1.7 SEQUENCING

1.7.1 Caisson Excavation

Perform excavation of caissons or groups of caissons so that reinforcing steel and concrete placement is a continuous operation performed the same day that the excavation is completed. Do not leave excavations open overnight.

1.7.2 Acceptance

Place concrete within 3 hours after approval of the completed excavation.

PART 2 PRODUCTS

2.1 MATERIALS

2.1.1 Concrete Work

Perform all concrete work in accordance with requirements of Section 03 30 00 CAST-IN-PLACE CONCRETE, as modified herein:

2.1.1.1 Strength

Provide concrete in accordance with 03 30 00 CAST-IN-PLACE CONCRETE.

2.1.1.2 Coarse Aggregate

Provide coarse aggregate in accordance with 03 30 00 CAST-IN-PLACE CONCRETE.

2.1.1.3 Reinforcing Steel

Provide reinforcing steel conforming to ASTM A615/A615M Grade 60, welded into cages in accordance with AWS D1.4/D1.4M and inserted securely in the caissons, in position and alignment, as shown, prior to concrete placement .

2.1.2 Welding

Perform shop and field welding in accordance with AWS D1.1/D1.1M. Provide certification of qualification of welding procedures, welders, and welding operators in accordance with

AWS D1.1/D1.1M. Keep records of test results of welding procedures not prequalified and copies of records for each qualified welding operator, containing records on positions of welding and types of electrode qualifications, and make available for examination by the Contracting Officer.

2.1.3 Casing Steel

ASTM A36/A36M. Provide zinc coating of casing steel conforming to **ASTM A123/A123M.** Provide casings with an outside diameters not less than indicated shaft sizes and a minimum thickness as required.

2.2 CAISSON DRILLING EQUIPMENT

Provide caisson drilling equipment with minimum torque capacity and downward force capacity suitable for the site conditions.

PART 3 EXECUTION

3.1 PREPARATION

Excavate **caissons** to established depths and dimensions shown; clean bottoms of caissons free of loose or soft material; level caissons; and dispose of excavated material in accordance with Section **31 00 00 EARTHWORK.** Submit a certified copy of the survey. Establish lines, levels, and caisson centerline locations, staked and maintained by a registered surveyor or engineer.

- a. When drilling caissons, protect the surrounding soil and the earth walls against cave-ins, displacement of the surrounding earth, and retention of ground water, by means of temporary steel casings. Provide casings with outside diameters not less than indicated shaft sizes, and a minimum of **1/4 inch** thick. Do not remove if the structural integrity of the caisson will be impaired, as determined by the Contracting Officer. Withdraw temporary steel casings as the concrete is being placed, maintaining sufficient head of concrete within the casing to prevent extraneous material from falling in from the sides and mixing with the concrete. Casings may be jerked upward a maximum of **4 inches** to break the bottom seal, but remove thereafter with a smooth, continuous motion.
- b. Thoroughly clean and oil the inside of steel casings before reuse.
- c. Leave the temporary casing in place from the caisson top to the ground surface until the concrete has set if the elevation of the top of the caisson is below the adjacent ground surface.
- d. Continuously remove all water that flows into the excavations and from the excavation bottom, to the extent possible, prior to concrete placement. The maximum permissible depth of water is **2 inches**. In the event of a severe water condition that makes it impossible or impractical to dewater the excavation, place concrete using an underwater tremie after water movement has stabilized.
- e. Each caisson excavation will be inspected and approved by the Contracting Officer prior to placing concrete. Keep a record of all inspections, with related construction changes. Provide support personnel for inspection and testing procedures.

3.2 INSTALLATION

- a. Continuously place concrete by methods that ensure against segregation and dislodging of excavation sidewalls, and completely fill the shaft. Place concrete by pumping or drop chutes in dry holes and by tremie or pumping in wet holes. Keep the discharge a minimum of **3 feet** below the fresh concrete surface during placement. Drilling of caissons or driving of casings must not be within **20 feet** of concrete placed within the last 3 days.
- b. Bring concrete to a true level surface inside the shaft and a full width cross key formed, or dowels installed, if it becomes necessary to interrupt placing concrete in any caisson. Prior to placing

additional concrete, clean surfaces of laitance and slush with one-to-one portland cement grout, having a water-cement ratio not exceeding that of the concrete.

- c. Place concrete in dry batter caissons with a drop chute extending within **3 feet** of the concrete surface in the excavation.
- d. Vibrate concrete for upper 10 feet of caisson.

3.3 TOLERANCES

- a. Correct any caisson out of center or plumb beyond the tolerance specified as necessary to comply with the tolerances. Any corrective cost is the responsibility of the Contractor.
- b. Make cross sections of shafts not less than design dimensions.
- c. Install caissons with top location deviating a maximum of **3 inches** from centerline locations.
- d. Install vertical caissons plumb within a maximum of **1-1/2 inches** for the first **10 feet** and within **1/2 inch** for each **10 feet** of additional depth.

3.4 PROTECTION

Provide protection around top of the excavation to prevent debris from being dislodged into the excavation and concrete.

3.5 RECORDS

Keep and submit complete, detailed and accurate records for each caisson installation. Include locations, shaft diameters, top and bottom elevations, depths of test holes, casing dimensions, concrete strength, concrete volume, quantity of rock excavation, excavation condition, dates of excavation and concrete placement, bearing strata description, and subsurface water conditions. Base location on the survey of the registered surveys or engineer provided by the Contractor. Tabulate all records, including corrective measures. Upon completion of caisson work, provide a record of centerline locations based on the survey of the registered surveyor or engineer provided by the Contractor. In addition, also record corrective measures. Deliver a complete tabulation of all records pertaining to approved caissons to the Contracting Officer.

-- End of Section --

SECTION TABLE OF CONTENTS

DIVISION 41 - MATERIAL PROCESSING AND HANDLING EQUIPMENT

SECTION 41 22 13.15

BRIDGE CRANES, OVERHEAD ELECTRIC, UNDER RUNNING TROLLEY

PART 1 GENERAL

- 1.1 REFERENCES
- 1.2 DEFINITIONS
- 1.3 SYSTEM DESCRIPTION
 - 1.3.1 Crane Design Criteria
 - 1.3.1.1 General
 - 1.3.1.2 Classification
 - 1.3.1.3 Rated Speeds
- 1.4 VERIFICATION OF DIMENSIONS
- 1.5 SUBMITTALS
- 1.6 QUALITY ASSURANCE
 - 1.6.1 Manufacturer Qualification
 - 1.6.2 Pre-Delivery Inspections
 - 1.6.2.1 Hook Proof Test
 - 1.6.2.2 Inspection of Hook Assembly
 - 1.6.3 Drawings: Overhead Electric Crane System
 - 1.6.4 Design Data: Load and Sizing Calculations
 - 1.6.5 Certificates
 - 1.6.6 Welding Qualifications and Procedure
- 1.7 CRANE SAFETY

PART 2 PRODUCTS

- 2.1 MATERIALS
 - 2.1.1 General
 - 2.1.2 Nameplates
 - 2.1.3 Capacity Marking
 - 2.1.4 Safety Warnings
- 2.2 STRUCTURAL REQUIREMENTS
 - 2.2.1 Structural Connections
 - 2.2.2 Crane Bridge Girder
 - 2.2.3 Bridge End Trucks
 - 2.2.4 End Stops
 - 2.2.5 Bumpers
 - 2.2.6 Crane Runway System
- 2.3 MECHANICAL REQUIREMENTS
 - 2.3.1 Threaded Fasteners
 - 2.3.2 Hoist
 - 2.3.2.1 Hoist Brakes
 - 2.3.2.2 Load Block and Hook
 - 2.3.2.3 Hoisting Rope
 - 2.3.2.4 Drum
 - 2.3.2.5 Sheaves
 - 2.3.3 Travel Drives
 - 2.3.3.1 Trolley Drives

- 2.3.3.2 Bridge Drives
 - 2.3.3.2.1 Bridge Travel Gearing
 - 2.3.3.2.1.1 Bridge Travel Reducer
 - 2.3.3.2.1.2 Bridge Open Gearing
- 2.3.4 Travel Brakes
 - 2.3.4.1 Trolley Brake
 - 2.3.4.2 Bridge Brake
- 2.4 ELECTRICAL REQUIREMENTS
 - 2.4.1 Motors
 - 2.4.2 Controls
 - 2.4.3 Protection
 - 2.4.3.1 Conductors
 - 2.4.4 Resistors
 - 2.4.5 Transients and Harmonics Protection
 - 2.4.6 Limit Switches
 - 2.4.7 Operator Controls
 - 2.4.7.1 Pendant Pushbutton Station
 - 2.4.7.1.1 Pendant Conductor System
 - 2.4.8 Electrification Systems
 - 2.4.8.1 Runway Conductor System
 - 2.4.8.2 Bridge Conductor System
 - 2.4.9 Overload Protection
 - 2.4.10 Enclosures
 - 2.4.11 Warning Devices
- 2.5 PAINTING SYSTEM
- 2.6 IDENTIFICATION PLATES
 - 2.6.1 Markings on Crane, Trolley, and Hook
- 2.7 ELECTRICAL ASSEMBLY

*AM0003

AM0003*

PART 3 EXECUTION

- 3.1 EXAMINATION
- 3.2 SHOP ASSEMBLY AND TESTS
- 3.3 ERECTION AND INSTALLATION
 - 3.3.1 Mechanical Alignment
 - 3.3.2 Electrical Adjustments
 - 3.3.3 Field Welding
 - 3.3.4 Field Painting
- 3.4 FIELD QUALITY CONTROL
 - 3.4.1 Post-Erection Inspection
 - 3.4.2 Operational Tests
 - 3.4.2.1 No-Load Test
 - 3.4.3 Test Data
 - 3.4.4 Hook Tram Measurement
 - 3.4.5 Load Tests
 - 3.4.5.1 Wire Rope Run-In
 - 3.4.5.2 Rated Load Test
 - 3.4.5.2.1 Hoist
 - 3.4.5.2.2 Trolley
 - 3.4.5.2.3 Bridge
 - 3.4.5.2.4 Trolley Loss of Power Test
 - 3.4.5.2.5 Bridge Loss of Power Test
 - 3.4.5.3 Overload Test
 - 3.4.5.3.1 Hoist
 - 3.4.5.3.2 Trolley
 - 3.4.5.3.3 Bridge
- 3.5 MANUFACTURER'S FIELD SERVICE REPRESENTATIVE
- 3.6 OPERATION AND MAINTENANCE MANUALS
- 3.7 FIELD TRAINING

3.8 FINAL ACCEPTANCE

-- End of Section Table of Contents --

SECTION 41 22 13.15

BRIDGE CRANES, OVERHEAD ELECTRIC, UNDER RUNNING TROLLEY

PART 1 GENERAL

1.1 REFERENCES

The publications listed below form a part of this specification to the extent referenced. The publications are referred to within the text by the basic designation only.

AMERICAN GEAR MANUFACTURERS ASSOCIATION (AGMA)

AGMA 908	(1989B; R 1999) Information Sheet: Geometry Factors for Determining the Pitting Resistance and Bending Strength of Spur, Helical and Herringbone Gear Teeth
ANSI/AGMA 2001	(2004D; R 2010) Fundamental Rating Factors and Calculation Methods for Involute Spur and Helical Gear Teeth
ANSI/AGMA 2015-1	(2001A; R 2014) Accuracy Classification System - Tangential Measurements for Cylindrical Gears
ANSI/AGMA 6013	(2006A; R 2016) Standard for Industrial Enclosed Gear Drives

AMERICAN INSTITUTE OF STEEL CONSTRUCTION (AISC)

AISC 360	(2016) Specification for Structural Steel Buildings
----------	---

AMERICAN SOCIETY OF MECHANICAL ENGINEERS (ASME)

ASME B1.1	(2024) Unified Inch Screw Threads (UN, UNR, and UNJ Thread Form)
ASME B30.10	(2019) Hooks
ASME B30.16	(2022) Overhead Underhung and Stationary Hoists
ASME B30.17	(2020) Overhead and Gantry Cranes (Top Running Bridge, Single Girder, Underhung Hoists)
ASME B30.30	(2019) Ropes
ASME HST-1	(2023) Performance Standard for Electric Chain Hoists
ASME HST-4	(2021) Performance Standard for Overhead Electric Wire Rope Hoists

AMERICAN WELDING SOCIETY (AWS)

AWS D1.1/D1.1M	(2020; Errata 1 2021) Structural Welding Code - Steel
AWS D14.1/D14.1M	(2019) Specification for Welding of Industrial and Mill Cranes and Other Material Handling Equipment

ASTM INTERNATIONAL (ASTM)

ASTM A1023/A1023M	(2021) Standard Specification for Stranded Carbon Steel Wire Ropes for General Purposes
ASTM F436/F436M	(2019) Standard Specification for Hardened Steel Washers Inch and Metric Dimensions
ASTM F3125/F3125M	(2019) Standard Specification for High Strength Structural Bolts and Assemblies, Steel and Alloy Steel, Heat Treated, Inch Dimensions 120 ksi and 150 ksi Minimum Tensile Strength, and Metric Dimensions 830 MPa and 1040 MPa Minimum Tensile Strength

BRITISH STANDARDS INSTITUTION (BSI)

BS ISO 4309	(2017) Cranes - Wire Ropes - Care and Maintenance, Inspection and Discard
-------------	---

CRANE MANUFACTURERS ASSOCIATION OF AMERICA (CMAA)

CMAA 70	(2020) Specification for Top Running Bridge and Gantry Type Multiple Girder Electric Overhead Traveling Cranes
CMAA 74	(2020) Specifications for Single Girder Cranes

MATERIAL HANDLING INDUSTRY OF AMERICA (MHI)

MHI MH27.1	(2016) Specifications for Underhung Cranes and Monorail Systems
------------	---

NATIONAL ELECTRICAL CONTRACTORS ASSOCIATION (NECA)

NECA NEIS 1	(2015) Standard for Good Workmanship in Electrical Construction
-------------	---

NATIONAL ELECTRICAL MANUFACTURERS ASSOCIATION (NEMA)

NEMA 250	(2020) Enclosures for Electrical Equipment (1000 Volts Maximum)
NEMA ICS 3	(2005; R 2010) Medium-Voltage Controllers Rated 2001 to 7200 V AC
NEMA ICS 5	(2017) Industrial Control and Systems: Control Circuit and Pilot Devices
NEMA ICS 6	(1993; R 2016) Industrial Control and Systems: Enclosures
NEMA ICS 8	(2011) Crane and Hoist Controllers
NEMA MG 1	(2021) Motors and Generators

NATIONAL FIRE PROTECTION ASSOCIATION (NFPA)

NFPA 70	(2023; ERTA 1 2024; TIA 24-1) National Electrical Code
---------	--

RESEARCH COUNCIL ON STRUCTURAL CONNECTIONS (RCSC)

RCSC A348 (2020) RCSC Specification for Structural Joints Using High-strength Bolts

SOCIETY FOR PROTECTIVE COATINGS (SSPC)

SSPC SP 6/NACE No.3 (2007) Commercial Blast Cleaning

SOCIETY OF AUTOMOTIVE ENGINEERS INTERNATIONAL (SAE)

SAE J429 (2014) Mechanical and Material Requirements for Externally Threaded Fasteners

SAE J995 (2017) Mechanical and Material Requirements for Steel Nuts

U.S. GENERAL SERVICES ADMINISTRATION (GSA)

FS RR-W-410 (2022; Rev J) Wire Rope and Strand

U.S. NATIONAL ARCHIVES AND RECORDS ADMINISTRATION (NARA)

29 CFR 1910 Occupational Safety and Health Standards

29 CFR 1910.147 The Control of Hazardous Energy (Lock Out/Tag Out)

29 CFR 1910.179 Overhead and Gantry Cranes

29 CFR 1910.306 Specific Purpose Equipment and Installations

UNDERWRITERS LABORATORIES (UL)

UL 943 (2016; Reprint Sep 2023) UL Standard for Safety Ground-Fault Circuit-Interrupters

UL 1004-1 (2012; Reprint Nov 2020) UL Standard for Safety Rotating Electrical Machines - General Requirements

1.2 DEFINITIONS

- a. Crane Bridge: That part of an overhead crane system consisting of a girder, end trucks, walkway, and drive mechanism which carries the trolley(s) and travels along the runway rails parallel to the runway.
- b. Crane Runway: The track system along which the crane operates horizontally, including track hangar rods, track connection devices, and runway structural supports.
- c. Dead Loads: The weight of all effective parts of the bridge structure, the machinery parts, and the fixed equipment supported by the structure.
- d. Crane Bridge Girder: The principal horizontal beam of the crane bridge structure. It is supported by the crane end trucks. Typically for single girder cranes the trolley mounted hoist is suspended from the girder below the crane.
- e. Lifted Load: The load consisting of the rated load and the weight of lifting devices attached to the crane such as the load block, bucket, or other supplemental devices.
- f. Original Equipment Manufacturer (OEM): the Company that produced the part or original

equipment.

- g. Packaged Hoist: A commercially designed and mass produced hoist characterized by the motor, gearing, brake(s), and drum contained in a single package often connected by the use of c, d, or p-face flanges.
- h. Patented Track: A generic term referring to track built in accordance with MHI MH27.1 utilizing a composite track section incorporating a proprietary bottom flange shape. For this crane system, it is provided for the crane bridge girder and also the crane runway track, if under running.
- i. Pendant: A control for a hoist and a crane. The pendant hangs from the hoist or the crane by a cable at a height that is easy for the operator to reach.
- j. Rated Load: The maximum working load suspended under the load hook.
- k. Standard Commercial Cataloged Product: A product which is currently being sold, or previously has been sold, in substantial quantities to the general public, industry or Government in the course of normal business operations. Models, samples, prototypes or experimental units do not meet this definition. The term "cataloged" as specified in this section is defined as "appearing on the manufacturer's published product data sheets. These data sheets must have been published or copyrighted prior to the issue date of this solicitation and have a document identification number or bulletin number.
- l. Trolley Load: The weight of the trolley and its associated equipment carried by the trolley wheels.
- m. Under running (Underhung) Crane: An electric overhead traveling crane that is supported by crane end trucks suspended below the crane runway. The load is supported by hanging from the lower flange of a beam or patented track.

1.3 SYSTEM DESCRIPTION

The requirements for the structures supporting the crane runway are specified in Section 05 12 00 STRUCTURAL STEEL, and must conform to AISC 360.

1.3.1 Crane Design Criteria

Cranes will operate in the given spaces and match the runway dimensions and rails indicated. Hook coverage, hook lift, clearances, lifting capacity, and load test weight must not be less than that indicated. Provide loaded hook coverage to the maximum extent possible.

1.3.1.1 General

Include the following: Number of cranes 1, located in building identified as Ebbing F-35 3-Bay Hangar, hoist bay, with the capacity expressed in 5 tons, for each crane. Also clearly locate and identify each hoist and system components.

1.3.1.2 Classification

Provide under running single girder electric bridge crane(s), with under running trolley mounted hoist, conforming to CMAA 74 service class C, as applicable. The crane(s) must be designed for operation in an indoor environment, general purpose service, meeting the requirements of ASME B30.16 and ASME B30.17, with an ambient temperature range of 50 to 97 degrees Fahrenheit. The crane(s) must operate in an NFPA 704 Class I, Division 2, Group D hazardous area. Hazardous protection is required from the finished floor level up to 1.5 feet above ground level and a 5 foot envelope around the aircraft. The total crane span must be as shown on the Drawings feet with a minimum vertical hook lift of 22 and as specified herein. Provide runways for multiple span cranes equally spaced apart.

*AM0003

AM0003*

The crane must be radio controlled and operate in the spaces and within the loading conditions indicated. Provide a crane, including hooks and hoisting rope or load chain, that is able to clear

permanent obstructions in all operating configurations. The crane must operate on 460-volts AC, 60 Hz , three phase power source. Maximum loading on the facility (without impact) due to dead loads, trolley loads, and lifted loads, with the trolley in any position, must not exceed the allowable wheel loading and wheel spacing of the facility (or not exceed maximum hanger loading for under running cranes).

***AM0003** 1.3.1.3 Rated Speeds

Provide the crane with rated (maximum) speeds within plus or minus 10 percent (in **feet/min**) for the main hoist, bridge, and trolley at the rated load as specified in the table below. The minimum speed must not exceed the values listed.

Rated Speeds feet/min		
Description	Minimum	Maximum
Main Hoist	0	~~4.75~~ <u>20</u>
Trolley	0	~~4.75~~ <u>80</u>
Bridge	0	~~4.75~~ <u>100</u>

The hook lift capacity and speed must be the manufacturer's standard within the limits specified.

AM0003*

1.4 VERIFICATION OF DIMENSIONS

The Contractor is responsible for the coordination and proper relation of their work to the building structure and to the work of all trades. Coordinate with the crane support structure design, where applicable, to provide the desired crane operating envelope (i.e., hook envelope and hook height). Verify all dimensions of the building that relate to fabrication of the crane and notify the Contracting Officer of any discrepancy before finalizing the crane order.

1.5 SUBMITTALS

Government approval is required for submittals with a "G" or "S" classification. Submittals not having a "G" or "S" classification are for information only. When used, a code following the "G" classification identifies the office that will review the submittal for the Government. Submit the following in accordance with Section **01 33 00** SUBMITTAL PROCEDURES:

SD-02 Shop Drawings

Overhead Electric Crane System; G,DO

Complete Schematic Wiring Diagram; G

SD-03 Product Data

Hoist Brakes; G

Travel Brakes; G

Load Block and Hook; G

Hoist and Trolley Units; G

Hoisting Rope; G

Travel Reducer; G
Bridge End Trucks; G
Crane Bridge Girder; G, DO
End Stops; G
Bumpers; G
Crane Runway System; G, DO
Motors; G
Enclosures; G
Circuit Breakers; G
Disconnect Switch; G
Contactors and Relays; G
Fuses; G
Variable Frequency Drives; G
Limit Switches; G
Resistors; G
Pendant Push-Button Station; G
Pendant Conductor System; G
Crane Controllers; G
Control Parameter Settings; G
Warning Devices; G
Runway Conductor System; G
Bridge Conductor System; G
Overload Protection; G
Painting System; G

SD-05 Design Data

Load and Sizing Calculations; G, DO

SD-06 Test Reports

Hook Proof Test; G
Post-Erection Inspection; G

Operational Tests; G

Hook Tram Measurement; G

Load Tests; G

SD-07 Certificates

Wire Rope; G

Crane Runway; G

Hazardous Material; G

Loss of Power Test; G

Overload Test; G

Brake Adjustment Record; G

Contractor Hazardous Environment; G

SD-10 Operation and Maintenance Data

Operation and Maintenance Manuals, Data Package 3; G

1.6 QUALITY ASSURANCE

1.6.1 Manufacturer Qualification

Overhead Electric Crane System, including sub-system components manufactured by vendors, must be designed by, or directly supervised by, a registered professional engineer (PE). PE licensing must be by a board or agency authorized to license and register professional engineers. The PE may be a Contractor's regular employee or a consultant. The PE's review and attestation of specification compliance and professional responsibility must be signified by their PE original seal and dated signature on the final drawings. The professional engineers must only undertake and perform work under this contract in the branch(s) of engineering in which they are licensed.

1.6.2 Pre-Delivery Inspections

Contractor is responsible for performance of quality control inspections, testing, and documentation.

1.6.2.1 Hook Proof Test

Proof test custom designed or non-ferrous load hooks per **ASME B30.10**. Perform the proof test prior to Hook NDT.

1.6.2.2 Inspection of Hook Assembly

Inspect hook prior to delivery. Furnish documentation of hook inspection to Contracting Officer prior to field operational testing.

Acceptance standard is no defects. A defect is defined as a linear indication for which the largest dimension is greater than **1/16 inch** long. Welding repairs of hooks are not permitted. A hook showing linear indications, damage, or deformation is not acceptable.

1.6.3 Drawings: Overhead Electric Crane System

- a. Submit drawings showing the general arrangement of all components in plan, elevation, and end

views to demonstrate proper interface with the facility and relation to other cranes on the same rail system, if applicable. Show all major features of the crane including: hook approaches on all four sides, clearances and principal dimensions, hoist, trolley and bridge drives, motor nameplate data, overcurrent protective device ratings, and electrical schematic drawings. Include weights and centers of gravity of major components (e.g., bridge girder(s), trolley/hoist).

- b. Submit shop drawings of all fabricated components. Shop drawing quality must be equivalent to the contract drawings accompanying this solicitation. Drawings must be reviewed, signed and sealed by a licensed professional engineer.
- c. Provide Bill of Materials for crane components on each drawing. The schedule must provide a cross reference between manufacturer data and shop drawings. Components listed on the schedule of crane components must include total quantity, description, original manufacturer, and part number. Distributing agents will not be acceptable in lieu of the original manufacturer.

1.6.4 Design Data: [Load and Sizing Calculations](#)

Submit complete list of equipment and materials, including manufacturer's descriptive data, technical literature, and performance charts and curves. Submit calculations reviewed, signed, and sealed by a registered professional engineer verifying the load cases, sizing of the bridge girder(s), end trucks, travel drives, motors, overcurrent protection, and conduit. Provide a list of all codes and standards, design assumptions, equations, specified efficiencies, limits, factors of safety, component ratings, and sources of values used. Include free body diagrams or sketches of each load case.

1.6.5 Certificates

All certifications must be dated and bear the original signature (above the printed name) of the authorized representative of the Contractor or the manufacturer of the items or equipment being certified. Submit certifications that clearly identify the crane, the drives, components, and location (as applicable) to which it applies:

- a. [Wire Rope](#) Certification with either the wire rope manufacturer's certification that the rope meets the published breaking force, or certification of the actual breaking force of a sample taken from the reel and tested. Show the published breaking force on the wire rope certificate; the actual wire rope breaking force must meet or exceed the published value. Certification must be traceable to the hoist, crane, and reel.
- b. [Crane Runway](#) Certificate stating that the new crane will operate properly on the runway. For runways provided by Contractor, include statement certifying runway has been aligned in accordance with [CMAA 74](#) or [MHI MH27.1](#), as applicable.
- c. [Hazardous Material](#) Certificate that the crane does not contain hazardous material including asbestos, lead, cadmium, chromium, PCBs, or elemental mercury. Products required for the designing and manufacturing of cranes must not contain the prohibited materials.
- d. [Loss of Power Test](#) Certificate stating that a test may be performed in which power is removed during operation without any detrimental effects to the crane.
- e. [Overload Test](#) Certificate stating that the crane can be periodically load tested to 125 percent (plus 0 minus 5 percent) of rated load.
- f. Certificate of the [Brake Adjustment Record](#). Provide a brake adjustment record and installation/maintenance manuals for each brake on the crane. Each brake measurement must have a tolerance traceable to the associated brake manual or documentation provided by the brake manufacturer, location of measurements, and the actual brake setting. Changes made to settings of the brake, at any time, will void the record.
- g. [Contractor Hazardous Environment Certificate](#) stating that the new crane and all associated components including the hoist are designed for operation in the hazardous environment

specified in the paragraph CLASSIFICATION.

1.6.6 Welding Qualifications and Procedure

Welding must be in accordance with qualified procedures using AWS D14.1/D14.1M as modified. Written welding procedures must specify the Contractor's standard dimensional tolerances for deviation from camber and sweep and not exceed those specified in AWS D14.1/D14.1M, MHI MH27.1 and CMAA 74. Welders and welding operators must be qualified in accordance with AWS D1.1/D1.1M or AWS D14.1/D14.1M.

1.7 CRANE SAFETY

Comply with the mandatory and advisory safety requirements of ASME B30.10, ASME B30.16, ASME B30.17, ASME HST-4 or ASME HST-1, 29 CFR 1910.147, 29 CFR 1910.179, 29 CFR 1910.306, and all applicable provisions of 29 CFR 1910 and NFPA 70.

PART 2 PRODUCTS

2.1 MATERIALS

2.1.1 General

Provide materials and equipment which are standard products of manufacturers regularly engaged in the fabrication of complete and totally functional cranes including necessary ancillary equipment. Material will be free from defects and imperfections that might affect the serviceability and appearance of the finished product. All material must be new and unused.

2.1.2 Nameplates

Secure nameplates to each major component of equipment with the manufacturer's name, address, type or style, model or catalog number, and serial number. Provide two bridge identification plates, one for each side of the bridge. Provide noncorrosive metal identification plates with letters which are easily read from the floor, showing a separate number such as BC-1, BC-2, for each bridge crane.

2.1.3 Capacity Marking

Mark the rated capacity in pound units on each side of the crane on the bridge girder. Capacity marks must be large enough to be clearly visible from the floor. Individual hoist units must have their rated capacity clearly marked on their lower block, and additionally labeled on the hoist body.

2.1.4 Safety Warnings

Affix labels in a readable position to each lift block or control station in accordance with ASME B30.16 and ASME B30.17. Submit safety warnings, diagrams and other instructions suitably framed and protected for display as indicated by the Contracting Officer as follows:

Design and locate the word "WARNING" or other legend to bring the label to the attention of the operator. Provide durable type warning labels and display the following information concerning safe-operating procedures: Cautionary language against lifting more than the rated load; operating the hoist when the hook is not centered under the hoist; operating hoist with twisted, kinked or damaged rope; operating damaged or malfunctioning hoist; operating a rope hoist with a rope that is not properly seated in its hoist drum groove; lifting people; lifting loads over people; and removing or obscuring the warning label.

2.2 STRUCTURAL REQUIREMENTS

Structural requirements must be in accordance with CMAA 74 and MHI MH27.1, as applicable. Structural steel materials must conform to the standards permitted in CMAA 74, MHI MH27.1, and AISC 360. Skewing and other applicable lateral loads must be considered in the design.

2.2.1 Structural Connections

High-strength bolted structural connections must be designed and installed in accordance with [RCSC A348](#). Bolts must be of [ASTM F3125/F3125M](#) Grade A325/A325M or Grade A490/A490M material. Galvanized bolts are not acceptable.

Welded connections for the crane must be performed in accordance with [AWS D14.1/D14.1M](#). Welded connections to the building must be performed in accordance with [AWS D1.1/D1.1M](#). Allowable stress values must comply with [CMAA 74](#) or [MHI MH27.1](#), as applicable.

2.2.2 Crane Bridge Girder

- a. Provide crane bridge girder(s) of rolled steel shape conforming to [CMAA 74](#) or patented track conforming to [MHI MH27.1](#). Intermittent ("skip") welds on bridge girder elements (e.g., web and flange interfaces) are prohibited. If the girder is notched to fit over the end trucks, reinforce the girder ends with vertical and horizontal stiffeners. Splices in the unsupported length of the girder are prohibited.
- b. For patented track girder(s), submit manufacturer's standard published tables that verify the crane bridge girder is sized in compliance with all specification requirements. When standard published tables are not available, provide calculations for the strength design and deflection of the bridge. Patented track girder must be of welded steel construction and fabricated by a manufacturer regularly engaged in the production of this type of beam.
- c. Keep splices in the bridge girder(s) to a minimum and splices in high stress locations must be avoided. Make splices with complete joint penetration welds. Field (on-site) welded splices are prohibited.

2.2.3 Bridge End Trucks

Provide bridge end trucks conforming to [ASME B30.17](#) and [CMAA 74](#) or [MHI MH27.1](#), as applicable. Configure end trucks with a feature that limits end truck movement to [one inch](#) in the event of wheel or shaft failure.

2.2.4 End Stops

Fit the crane bridge girder(s) with structural steel end stops. Locate stops to permit maximum trolley travel. Design end stops in accordance with [MHI MH27.1](#) and [ASME B30.17](#). Provide a system in which the travel wheels do not contact the end stops. End stops must be designed to absorb the maximum kinetic energy and impact force developed by the bumper contact. Provide end stops compatible with trolley bumpers and designed to bolt to the crane bridge girder.

2.2.5 Bumpers

Fit bridge end trucks and trolley frames with shock-absorbing bumpers capable of decelerating and stopping the bridge and trolley within the limits stated by [ASME B30.17](#). Ensure bumpers conform to [ASME B30.17](#). Bumpers must fully engage end stops. Mount bumpers so that there is no direct shear on mounting bolts (if any) upon impact. Bumpers must provide adequate clearance between the crane and surrounding structure when compressed to preclude damaging equipment (clearance requirements are defined in [MHI MH27.1](#) or [CMAA 74](#), as applicable, and [ASME B30.17](#)). When more than one crane is located and operated on the same runway, bumpers must be provided on their adjacent ends or on one end of one crane. Fit the other end of the end-truck with a structural steel stop to engage the bumpers of the adjacent crane. Ensure bridge bumpers are properly aligned with runway end stops.

2.2.6 Crane Runway System

- a. Provide the complete runway track suspension system that is required to hang the crane runway

track at its indicated location from the structural supports indicated on the drawings. Provide runway and support structure for under running crane of rolled steel shapes conforming to [CMAA 74](#) or patented track girders conforming to [MHI MH27.1](#).

- b. For rolled steel shapes, locate splices under structural support members.
- c. For patented track girders, perform splices as necessary in accordance with the manufacturer's recommendations and requirements. Align ends of lower T-section to minimize the horizontal gap on the running surface to not greater than [1/16 inch](#) and not greater than a vertical difference of [1/32 inch](#) for the wheel running surface alignment for a smooth crossing by the wheels. Splice assemblies must be from the same manufacturer as the patented track and located under structural support members. When runways are suspended, bracing preventing damaging lateral or longitudinal movement is required. Loads transmitted to the building through the suspension must have the review and approval of the building engineer of record (EOR) prior to installation. Submit manufacturer's standard published tables that verify the crane runway track is sized in compliance with all specification requirements. When standard published tables are not available, provide calculations for the strength design and deflection of the beams.
- d. Runway support structure must be designed, fabricated, and installed such that runway rails meet the alignment tolerances of [CMAA 74](#) or [MHI MH27.1](#), as applicable. Provide means to allow for vertical adjustment of the runway track both before and after the system has been put in operation so that track can be erected and maintained level. Brace runway to restrain the track against damaging lateral and longitudinal movements. Where the runway track is suspended from hanger rods, provide means preventing the hanger rod nuts from backing off the rods. Allowable stress in hanger rods is 20 percent of the minimum specified ultimate strength of the material used.
- e. For under running crane runways, design, fabricate, and install new runway end stops in accordance with [ASME B30.17](#) and [CMAA 74](#) or [MHI MH27.1](#), as applicable. End stops must be designed to absorb the maximum kinetic energy and impact force developed by the bumper contact. Provide end stops compatible with end truck bumpers, designed to bolt to the runway support girders, and maximize bridge travel.

2.3 MECHANICAL REQUIREMENTS

- a. Provide steel shafts, gears, and keys, with the exception of worm gears which may be bronze. No three or more bearing shaft configurations are allowed.
- b. Cast iron and aluminum used to support components of the hoist power transmission train must be ductile. For the purposes of this specification, "ductile" is defined as having a minimum elongation of 5 percent in 2.00 inches.
- c. Provide steel or ductile/malleable cast iron brake housings of motor mounted disc brakes, brake lining backing plates, shoes and shoe holders. Provide spring-set brake shoe or pad linings of a non-asbestos material.
- d. All mechanical components must be accurately aligned and positively secured to maintain the alignment. Parts must not be forced into position to obtain apparent alignment.
- e. Provide minimum bearing life in accordance with ASME hoist performance standards and [MHI MH27.1](#) or [CMAA 74](#), as applicable.

2.3.1 Threaded Fasteners

Fasten mechanical connections that are not part of a commercial packaged assembly with [SAE J429](#) Grade 5 fasteners, [ASTM F436/F436M](#) washers, and [SAE J995](#) Grade 5 nuts. Lubricate all mechanical fasteners unless otherwise specified by the original component manufacturer.

2.3.2 Hoist

Provide hoist conforming to **ASME B30.16**, except as modified and supplemented in this section. Packaged **hoist and trolley units** (packaged hoists) must be electric chain hoist conforming to **ASME HST-1** Duty Class H3 or better and be rated for the operating environment.

Configure trolley such that the trolley frame contacts the trolley stops and prevents the trolley from dropping more than one inch in the event of an axle or wheel failure.

2.3.2.1 Hoist Brakes

- a. Equip the hoist with two holding brakes, each with a minimum torque rating of 125 percent of the rated load hoisting torque. Provide a brake configuration with one electro-mechanical spring set brake and one mechanical load brake, or self-locking worm gear, that stops and holds 125 percent of the hoist's rated load and does not require the load to be raised before being lowered.
- b. Electro-mechanical brakes must have an externally accessible means of manual release.

2.3.2.2 Load Block and Hook

- a. **Provide a load block constructed of non-sparking materials. Covering the exposed surfaces of the load block with bronze, stainless steel, or aluminum covers attached with similar fasteners is acceptable.** The load block must be designed to prevent metal-to-metal contact of moving parts. The block must be fully enclosed, concealing the sheaves and wire ropes, except for wire rope slots and drain holes. The design must preclude the wire rope from being cut, pinched, crushed, or chafed in case of two-blocking. The design must preclude the load chain from being cut, pinched, crushed, or chafed in case of two-blocking. **Provide sprockets constructed of non-sparking metals in the load block.** Standard commercial blocks may be used at their published ratings when their published design factors are 5.0 or greater.
- b. Provide an unpainted and unplated forged steel single barbed hook with a minimum material longitudinal elongation of 16 percent in 2 inches. **Provide an unpainted and unplated single barbed hook of non-sparking material. Bronze clad hooks are prohibited.** Hooks must conform to the requirements of **ASME B30.10**. The hook must be a standard commercial product with a published design factor of 5.0 or greater. Fit hook with a safety latch designed to preclude inadvertent displacement of slings from the hook saddle. The hook and hook nut must be removable without unreeving of the hoist. Provide hook nut secured to the hook with a commercial standard removable and reusable means. Do not weld hook nut. When provided, provide shank and nut threads with a Class 1 or 2 fit, per **ASME B1.1**. **The hook nut must be of non-sparking materials.** Hook must be free to rotate through 360 degrees when supporting the test load up to 125 percent of the rated capacity. ~~Upper hooks of hook suspended hoists must be of non-sparking materials.~~

*AM0003

AM0003*

2.3.2.3 Hoisting Rope

- a. Wire rope must comply with **ASME B30.30** and **FS RR-W-410**, **ASTM A1023/A1023M**, or **BS ISO 4309** and have a rope classification appropriate for the usage. Wire ropes must be handled and seized in accordance with **ASME B30.30**. The wire rope must be in a double reeved configuration equalized with a sheave. Select wire rope minimum design factor in accordance with **ASME B30.16**. Provide proof of Wire Rope breaking force.

~~*AM0003 b. Provide hoist wire ropes with improved, extra-improved, or extra-extra-improved plow steel (or appropriate ISO grades), pre-formed, regular lay, bright, and uncoated, with an independent wire rope, wire strand, or otherwise, steel core. Hot dipped galvanized wire rope is not permitted.~~

- ~~eb.~~ **Wire rope must be spark resistant. Provide stainless steel hoist ropes with an independent wire rope, wire strand, or otherwise, steel core.**

AM0003*

2.3.2.4 Drum

Provide grooved drum made of steel. Design drum in accordance with [ASME B30.16](#). All hoisting rope is to be wound in a single layer and provided with no less than two dead wraps of hoisting rope remaining at each anchorage when the hook is in its extreme low position.

2.3.2.5 Sheaves

Provide steel sheaves. [Provide sheaves constructed of non-sparking metals in the load block](#). Size sheaves in accordance with [ASME B30.16](#) for the minimum pitch diameters of running and equalizer sheaves.

2.3.3 Travel Drives

Provide under running travel assemblies with a minimum of one driven wheel on each side of the web and at least one quarter of all wheels driven.

The travel drive arrangement must consist of motor(s) driving through self-contained gear reduction units located at each driven wheel assembly. Gear reducers must be fully enclosed in an oil-tight housing and provided with a convenient means of lubricant level indication and draining. Open-type gearing is not acceptable, except for final drives.

2.3.3.1 Trolley Drives

Provide a motor-driven trolley arrangement. Acceleration and deceleration must meet the requirements specified in [CMAA 70](#). Provide trolley travel limit switches.

2.3.3.2 Bridge Drives

Provide a motor-driven bridge arrangement. Acceleration and deceleration must meet the requirements specified in [CMAA 74](#). Provide bridge travel limit switches.

2.3.3.2.1 Bridge Travel Gearing

Gearing must conform to [ANSI/AGMA 2001](#) and [AGMA 908](#), with internal and external gear dimensional tolerances conforming to the applicable AGMA standard for tooth geometry and tolerances.

2.3.3.2.1.1 Bridge [Travel Reducer](#)

Gear reducers must be standard commercial products designed, manufactured, and rated in accordance with [ANSI/AGMA 6013](#). Provide cranes with a CMAA service class "C" or higher with the corresponding "Industrial Duty" service factors. The speed reducer input (high speed) gear set must use helical (including double helical and herringbone), spiral bevel, or worm gear tooth forms. Provide torque arms that are not of the threaded rod type. Operation must be smooth and quiet.

2.3.3.2.1.2 Bridge Open Gearing

Provide all gears and pinions with adequate strength and durability for the crane service class and manufactured to [ANSI/AGMA 2015-1](#) Accuracy Grade A8 or better. Wherever feasible, open gears must be enclosed with safety guards provided with openings with covers for inspection and access for grease lubrication.

2.3.4 [Travel Brakes](#)

Provide travel drives with an end-mounted electro-mechanical spring set brake conforming to the requirements of [CMAA 74](#) or non-freecoasting mechanical drive capable of stopping the motion of the travel function within a distance in [feet](#) equal to 10 percent of the full load speed in [feet](#) per minute when traveling at full speed with a full load.

Spring set brakes must be provided with an externally accessible means to manually release the brake.

2.3.4.1 Trolley Brake

Provide brakes for underrunning trolleys/carriers sized in accordance with [ASME B30.17](#), but not sized larger than 150 percent of the drive motor rated torque.

2.3.4.2 Bridge Brake

Provide brakes with a minimum torque rating per [CMAA 74](#) according to the applicable environment, but not sized larger than 150 percent of the drive motor rated torque.

2.4 ELECTRICAL REQUIREMENTS

- a. The design, selection, rating, and installation of the electrical portions of the crane and its accessories must conform to the requirements of [NEMA ICS 3](#), [NEMA ICS 8](#), the applicable ASME HST standard, and [NFPA 70](#), and other requirements specified herein.
- b. All electrical components must be industrial grade, commercially available and comply with established national or internationally recognized approving organizations such as Underwriters Laboratories (UL) and Canadian Standards Association (CSA). [All electrical components installed or operated in hazardous areas including but not limited to enclosures, junction boxes, disconnects, pendant controller, and electrification must be designed and rated for the NFPA 70 Hazardous Classifications specified in the paragraph CLASSIFICATION.](#)
- c. All electrical components must be located so they are easily accessible for inspection and maintenance without removing other parts, doors, or door center posts. Electrical equipment and panel wiring must be installed in a neat and workmanlike manner in accordance with Electrical Construction Standard [NECA NEIS 1](#). Each motion of the crane must be provided with a separate control system or drive. The loss of any one function must not prevent the operation of other unaffected functions. Two independent relays, contactors, drive inputs, or other equivalent components/logic must be utilized for each function to provide directional control such that the failure of a single relay/contactor/component cannot result in motion in an unintended direction.
- d. Disconnecting means for cranes must be in accordance with [NFPA 70](#) Article 610.32. A permanent placard must be installed on the face of the main line disconnect that states "WARNING – THIS DOES NOT ISOLATE POWER TO LIGHTING, RECEPTACLES, AND ANCILLARY EQUIPMENT". Additionally, a lighting (ancillary equipment) disconnect must be provided, with lockout feature, as the isolation means for the lighting transformer and lighting circuit breaker panel, which must power the crane's ancillary equipment. It must feed 480 VAC to the primary side of the transformer directly from the runway conductors via tapping the line side of the main power disconnect. Provide individual disconnects, with lockout feature, capable of being locked in the open position for bridge lights and receptacles.
- e. Unless otherwise specified, interconnecting wiring must be of copper stranded construction complying with Table 310.104(A) of [NFPA 70](#). Interconnecting wiring containing asbestos in the insulation or outer covering are prohibited. Aluminum conductors must not be used. Aluminum connectors are allowed if they are rated for use with copper conductors (marked "AL/CU"). All conductors connected to or routed above resistors must have insulation shown in [NFPA 70](#) Table 610.14(a) for [257 degrees F](#). For packaged hoists and hoist/trolleys, provide wiring sizes in accordance with [NFPA 70](#) Table 610.14(a). Motor branch circuit conductors not part of a packaged hoist and hoist/trolley must be sized as to have an ampacity not less than 150 percent of the motor full load current rating and to be no smaller than 12 AWG. Conductors must be selected and de-rated based on maximum ambient temperature. Continuous loads such as utility, heating, lighting, and air conditioning must be multiplied by 2.25 to determine ampacity in order to permit application of [NFPA 70](#) 610.14 (A) for crane supply conductors. Wire-nuts are not permitted on splices. However, connections for lighting ballasts may be made using wire-nuts (if applicable).

- f. Excluding conduit directly connected to dynamic breaking resistors, raceways must maintain a 12-inch clearance between the raceway and dynamic braking resistors. A separate grounding wire, sized in accordance with Section 250.122 of [NFPA 70](#), must be routed with all ungrounded conductors. Only one equipment grounding conductor must be run in each conduit and be the largest size required for any circuit routed in that conduit. All wiring must be numbered or tagged at all connection points. Power conductors which are shielded such that their wire size cannot be easily determined must be labeled as to the conductor size. All unused conduit openings must be plugged.
- g. When fiber optic cable is utilized, inspections and performance checks must be accomplished upon completion of on-site installation to ensure cable cleanliness and proper signal integrity. Testing and verification must be conducted by a knowledgeable fiber optics technician using specialized, calibrated equipment. Cables must be tested for signal loss/attenuation. The fiber optic system must also be tested using an Optical Time Domain Reflectometer (OTDR). Final attenuation and OTDR readings from each fiber optic cable run, including spares, must be documented as a baseline for future reference. All spare fiber optic cables must have protective covers over their ends to maintain cleanliness while not in use. When fiber optic cable is utilized the drive OEM's recommendations for encoders and optical to digital converters must be followed. All system components utilized for this purpose must have known compatibility prior to integration.
- h. Power cables and low voltage signal cables may not be mixed in the same conduit.
- i. The crane manufacturer must furnish and install all electrical equipment on the crane conforming to [NEMA ICS 6](#), including motors, conforming to [NEMA MG 1](#), electrically released brakes, switches, [crane controllers](#), panels, operating station, wiring system, cables, and crane electrification.

2.4.1 [Motors](#)

Motors must meet all applicable requirements of [NEMA MG 1](#) and [UL 1004-1](#). [CMAA 70](#) calculations for motor horsepower shall be used in selecting bridge, trolley, and hoist drive motors. All motors must have a minimum hoist duty rating H3 and be Totally Enclosed Non Ventilated (TENV), Totally Enclosed Fan Cooled (TEFC), or Totally Enclosed Blower Cooled (TEBC). Provide inverter duty motors for Open Loop [Variable Frequency Drives](#) (VFD). Provide motors with a minimum of Class F insulation. Provide motor overload protection utilizing a thermal sensitive device embedded in its windings.

2.4.2 Controls

- a. Provide static reversing, variable frequency drives (VFD) for the bridge, trolley and hoist electric controls. VFD controllers must meet [NEMA ICS 8](#), Part 8 and at a minimum, provide under-voltage protection, electronic instantaneous over current protection, DC bus over voltage protection, and be able to withstand output line to line shorts without component failure. Select bridge and trolley drives such that the continuous rating of the controller is not less than the calculated motor full load current based on [CMAA 70](#) paragraph 5.2.9.1.1.1 and [NFPA 70](#) Table 430.250. Select hoist drives such that the continuous rating of the controller is not less than 125 percent of the calculated motor full load current based on [CMAA 70](#) paragraph 5.2.9.1.1.1 and [NFPA 70](#) Table 430.250. All hoist drives must have a motor over-torque limit to lock out the hoist and prevent gross overload of the associated hoist. Provide dynamic braking for each electric drive that is sized per VFD manufacturer's requirements. Submit VFD [Control Parameter Settings](#).
- b. Provide speed control which is infinitely variable for each function, controlled via pendant pushbutton station. Provide controls designed such that the maximum speed of each function will be limited to 25 percent of rated speed when a slow speed switch is actuated on the controllers. Energize a yellow/amber light/indicator while in slow speed mode.

- c. The hoist, trolley, and bridge brakes must set after the associated controller decelerates the drive motor to a controlled stop. The hoist, trolley, and bridge, controllers must be sized to provide sufficient starting torque to initiate motion of that crane drive mechanism from standstill with 0 to 125 percent of rated load on the hook. The hoist controller must prove torque before release of the brakes and enable the drive motor to develop full torque continuously at zero speed. Motors must operate smoothly at all speeds without torque pulsations and must only be energized within the frequency range of 50-60 Hz at rated speed. The hoist control system may utilize overspeed up to 120hz, unloaded only, if the drivetrain equipment has all been balanced and is rated for the resulting speed.
- d. The use of definite purpose contactors is prohibited. If IEC contactors are used, the application cannot exceed the contactor manufacturer's AC3 ratings for the contactor at a minimum.
- e. On hoist function roll-up must be less than 1/8 inch measured at the hook block and roll-back must not occur over the entire load range.
- f. Use of Uninterruptible Power Supplies (UPS) is prohibited. Feed control circuits from a single phase, air cooled, double wound transformer with a grounded metal screen between the primary and secondary windings of the transformer.
- g. Provide a main line contactor. Energization of the main line contactor must be controlled by the POWER-OFF/POWER-ON switch/pushbutton on all controllers. Upon actuation of the POWER-OFF pushbutton; power to all drive motors, brakes, and controls must be removed. The mainline contactor must not be able to be energize while the POWER-OFF pushbutton is actuated. The POWER-OFF pushbutton circuitry must be independent of all controls or any other electronic devices.
- h. Provide a spring returned brake bypass keyswitch for each hoist. The switch allows for actuation of the electro-mechanical brake for independent testing of the mechanical load brake. The normal position allows both brakes to work in their normal operating configuration. Label the keyswitch positions as "NORMAL" and "LOAD BRAKE TEST".

2.4.3 Protection

Protection must not be less than that required by [NEMA ICS 3](#), [NEMA ICS 8](#), [CMAA 74](#), [NFPA 70](#), [UL 1004-1](#), [UL 943](#), [29 CFR 1910.147](#), [29 CFR 1910.179](#), [29 CFR 1910.306](#) and all applicable provisions of [29 CFR 1910](#). All protection must be by circuit breakers or fuses. Provide a [disconnect switch](#) or enclosed type circuit breaker readily accessible to the crane operator for the crane disconnect. Motor branch circuits must be individually protected by inverse time circuit breakers capable of being locked in the open position. The means for locking must remain in place with or without the lock installed. Motor full load current from [NFPA 70](#) Article 430, Part XIV (Tables) must be used to calculate the circuit breaker size.

Provide disconnecting means on the crane in accordance with [NFPA 70](#) Article 610.32. Provide for lockout/tagout of all hazardous energy sources. Provide product data for all [circuit breakers](#) and [fuses](#).

2.4.3.1 Conductors

- a. The crane contractor is responsible for ensuring that all conductors from the load side of the existing floor level disconnect to the motor branch circuits have adequate overcurrent protection complying with one of the following:
 - (1) Not be greater than the largest rating or setting of any branch circuit protective device plus the sum of the nameplate rating of all other loads per [NFPA 70](#) Article 610.41(A).
 - (2) Not be greater than the ampacity of all feeder conductors after all ampacity correction factors have been applied.
- b. Conductors for brake coils must be protected by fuses or other protective devices. The device

must be chosen to protect the brake circuit conductors from ground faults or short circuits.

2.4.4 Resistors

Provide resistors with natural convection cooling sized as recommended by the VFD OEM and fabricated of corrosion resistant metal; the use of "wire wound" type resistors is prohibited for segments of 8 ohms or less. Mount resistors in substantial, ventilated enclosures constructed entirely of non-combustible materials. Provide resistors with terminals fitted in the coolest position in the enclosure.

2.4.5 Transients and Harmonics Protection

- a. Provide **contactors and relays** with appropriate Metal Oxide Varistors (MOV) or resistor-capacitor (R-C) surge absorbers installed across the respective coil.
- b. Provide transient protection for electronic drive controllers that is either internal to the drive or via an MOV connected line-to-ground close to the line terminals of the drive.
- c. Provide line reactors rated for continuous duty operation based upon the motor nameplate amperes. With motors of 50 horsepower or greater, harmonics protection must be provided by an isolations transformer or as recommended by the VFD OEM. For a drive motor branch circuit that exceeds 150 feet in length, a reactor must also be connected in series with the controller load (output) terminals to provide standing wave protection or as otherwise recommended by the VFD or motor OEM.

2.4.6 Limit Switches

- a. Provide primary upper and lower geared limit switches. Geared limits must allow reversing direction to back out of the limit without resetting. The lower limit switch must be set such that there are a minimum of two wraps of rope on the hoist drum.
- b. Provide a backup mechanical hook block activated upper limit switch wired independent of the directional controllers and the primary upper limit switch that removes power from the hoist motor, hoist brake and hoist controls conforming to **NEMA ICS 5**. The backup limit must require hoist resetting prior to operation of the hoist in any direction.
- c. For chain hoists, the upper hoist limit switch must be wired to remove all power from the hoist drive motor and brake(s) independent of the microprocessor drive. A two-position spring-returned bypass switch must be provided that allows for resetting of the final limit switch prior to resuming operation. During resetting of the final limit, the hoist must operate in the lowering direction only.
- d. Travel limit switches must be provided for the bridge and trolley motion to slow the crane to 25 percent of its rated speed 10 feet before the bridge end stops and 5 feet from the trolley end stops. Limit switches must be mounted rigidly in a manner so as to protect the switch from misalignment or damage. The target/trip arm must be large enough to provide interception given a misalignment were to occur.

~~*AM0003 e. Limit switches must be rated for the NFPA 70 Hazardous Classifications specified in the CLASSIFICATION paragraph of this specification.~~

AM0003*

2.4.7 Operator Controls

- a. Provide crane equipped with a pendant pushbutton station .
- c. If VFD controls are not provided, provide directional contactors with both mechanical and electrical interlocks.
- d. "Operator controls must be rated **NEMA Type 7** for Class I, or **NEMA Type 9** for Class II according to the **NFPA 70** Hazardous Classifications specified in the **CLASSIFICATION** paragraph of this

specification."

2.4.7.1 Pendant Pushbutton Station

The cranes must be controlled from a pendant pushbutton station suspended from the trolley or an independent festooned messenger track system, operating the length of the bridge. Provide multiconductor flexible cords for pendant pushbutton stations with No. 16 AWG minimum conductors. Provide a method of strain relief to protect the electrical conductors from damage. Locate the pendant pushbutton station **4 feet** above the finished floor. Pushbutton pendant station must have its elements legibly marked and arranged vertically, in order, in accordance with **CMAA 74**. Provide 2-step infinitely variable pendant pushbuttons for control of the hoist, trolley, and bridge. Provide pendant pushbuttons for control that spring return to the OFF position. Voltage in the pendant pushbutton station must not exceed 150 Volts AC or 300 Volts DC. Provide a maintained two-position selector switch for slow speed selection. **The pendant must be rated for the NFPA 70 Hazardous Classifications specified in the CRANE DESIGN CRITERIA, sub- paragraph CLASSIFICATION.** Provide the pendant pushbutton station with a NEMA Type 7 for Class I, hazardous environments and NEMA Type 9 for Class II, hazardous environments, as classified by **NFPA 70**.

2.4.7.1.1 Pendant Conductor System

Provide a festoon type pendant conductor system. The festoon cables must be flat cables suspended from carriers riding on an I-beam or C-track. The pendant controller must be capable of traveling the entire length of the bridge and move independently of the trolley. Festoon loops must not extend below the high hook position.

2.4.8 Electrification Systems

2.4.8.1 Runway Conductor System

- a. Provide a rigid runway Conductor Bar System for the runway conductor system, including all necessary cables and hardware to the crane from a wall or column mounted disconnect switch. Provide electrification system with three power conductors and an equipment grounding conductor. The crane must be grounded through the runway electrification system. Provide runway conductors sized for simultaneous motions of the hoist, bridge, trolley mechanisms and any ancillary loads. If there is any way the hook block or wire rope can swing into the runway electrification, provide a guard installed to prevent contact.
- b. Provide two Collector Shoes (tandem design) for each conductor; each collector shoe must be rated for not less than the runway conductor sizing, so as to provide redundancy.

2.4.8.2 Bridge Conductor System

- a. Provide Festoon System for the bridge conductor system utilizing cables suspended from carriers riding on an I-beam or C-track. Conductors must be fabricated from copper. A minimum of 20 percent of the festoon control circuit conductors for each electrification system must be spares at the time of crane acceptance. The trolley is required to be grounded through this conductor system. Festooned cable loops must not extend low enough to come into contact with any obstructions.

2.4.9 Overload Protection

- a. Provide a capacity overload protective device for all hoist systems using VFD drive capacity overload protection (separate from torque limiting feature of the VFD). Set hoist capacity overload protection at 100 percent of rated capacity. Hoist capacity overload protection must be adjustable between 80 and 150 percent of hoist capacity. Provide a keyed override or other means to disable the hoist capacity overload protection when performing a load test. If a slip clutch is used as the overload limiting device, it must comply with all **ASME B30.16** requirements. Provide adjustable slip clutches set at or less than the cranes maximum test load. If the slip clutch is non-adjustable, the OEM factory setting is acceptable and must be

identified with the Product Data sheets and O&M manual.

- b. Initially, set the torque limiting capability of the VFD (that is separate from the capacity overload protective device) to 150 percent of the motor torque (amperage) necessary to hoist 100 percent load. It may be adjusted up only to avoid nuisance trips and adjusted down if possible while still avoiding nuisance trips.

2.4.10 Enclosures

- a. Provide enclosures for control panels, controls, and brakes in accordance with **NEMA 250** and **NEMA ICS 6**, Classification Type 3 outdoor, dust-tight, rain-tight, sleet-resistant .
- b. Provide a non-resettable hour meter, connected across the main line contactor, readable from the exterior of the main control panel, to indicate the elapsed number of hours the crane is energized.
- c. Gaskets of enclosures and fixtures, and joints and contact surfaces of hazardous/explosive enclosures must be kept free of any paint to prevent damage during removal and reinstallation of gaskets of enclosures.

2.4.11 Warning Devices

Provide a warning strobe light that is illuminated at all times during movement of the hoist, trolley, or bridge function, but may be deactivated on the operator control station.

2.5 PAINTING SYSTEM

- a. Remove all grease, oil, and surface debris by solvent wiping or detergent/water scrubbing, prior to blast cleaning. Prepare surfaces to be coated by abrasive blasting to **SSPC SP 6/NACE No.3**, Commercial Blast Cleaning, or in accordance with the coating manufacturer's requirements, whichever is more stringent.
- b. Use a painting system appropriate for the conditions provided in the Crane Design Criteria section of this specification. Paint exposed portions of the crane and crane runway system using a three-coat system as follows: zinc-rich primer consisting of a minimum of 77 percent zinc by weight in the dry film, an anticorrosive epoxy intermediate coat, and an aliphatic polyurethane top coat . All paint products must be supplied by a single manufacturer and free of chromates, lead, and mercury. Apply each coat in accordance with manufacturer's instructions and requirements. Ensure each coat is smooth, even, and free of runs, sags, orange peel, and other defects. Desired color of finish coat is brilliant yellow . Submit product data for painting system.
- c. Coat faying surfaces of bolted connections per **RCSC A348**, but do not apply finish paint.
- d. Paint the load block brilliant yellow with black diagonal striping.
- e. Paint, coatings, or galvanizing on the following items or areas is not acceptable: hoist wire rope or load chain, hooks, hook nuts, sheave and drum grooves, sprockets, wheel treads, lubrication fittings, nameplates, flange mounting faces, corrosion resistant steel, bronze, or other items not normally painted.
- f. Factory paint electrical and mechanical equipment in accordance with the manufacturer's best standard practice for the specified environment.

2.6 IDENTIFICATION PLATES

Furnish and install identification plates. Provide non-corrosive metal identification plates with clearly legible permanent lettering giving the manufacturer's name, model number, serial number, capacity in pound units, and other essential information or identification.

2.6.1 Markings on Crane, Trolley, and Hook

To avoid operation of the crane in the wrong direction, affix the appropriate directions (NORTH, SOUTH, EAST, and WEST) with arrows on both sides of the bridge and both sides of trolley, as applicable. Markings must be visible by the operator and from the loading point. Labels on the controls must have corresponding directional (NORTH, SOUTH, EAST, and WEST) markings. Markings must agree with the markings on controller. Do not indicate directional arrows on controller.

Mark the hook rated capacity in pound units on both sides of the hoist load block.

2.7 ELECTRICAL ASSEMBLY

Installation of all electrical wiring, conduit, and components must be performed in accordance with the requirements of **NFPA 70**. As a minimum, items a. through g. below must be followed:

- a. All electrical connections must be installed in accordance with **NFPA 70** Articles 110.14 or 430.9, as applicable, or as recommended by the device manufacturer.
- b. Crimped terminal lugs, if used, must be properly sized for the wire and installed using the device(s) – e.g., crimping tool and indenter – recommended by the terminal lug manufacturer.
- c. All spare conductors must be identified as spare conductors, and must have their ends insulated to preclude accidental contact with energized equipment.
- d. Bonding straps and equipment grounding conductors must be connected to engineered ground points, have all paint removed from their termination points, or have tooth lockwashers (star lockwashers) installed, to insure proper grounding of the equipment.
- e. Rigid Polyvinyl Chloride conduit may be used to protect festoon cable from physical damage when the cable is run along the footwalk of the crane, provided that only sections of conduit are used.
- f. Festoon cable must be installed with suitable strain relief and protected from physical damage in accordance **NFPA 70** Article 610.11(E)(1). This includes damage from chafing against the crane structure and any other type of damage that may be incurred.
- g. Fiber optic cable must be installed in accordance with the manufacturer's installation guidelines. However, at a minimum the following guidelines must be adhered to: no sharp bends (bend radii must be greater than 1 inch or as prescribed by the manufacturer), avoid tight loops, no zip ties, and no stretching of cable.

PART 3 EXECUTION

3.1 EXAMINATION

After becoming familiar with all details of the work, and before performing any work, verify all dimensions in the field. The Contractor is responsible for the coordination and proper relation of the contracted work to the building structure and to the work of all trades. Verify all dimensions of the building that relate to fabrication of the crane and notify the Contracting Officer of any discrepancy before finalizing the crane order.

3.2 SHOP ASSEMBLY AND TESTS

Shop assemble major components as completely as possible. Reeving of drums and sheaves is not advisable for shop testing, however it is acceptable for packaged hoists. Functionally test the crane system at the construction facility prior to shipment. The Government reserves the right to inspect the crane for compliance with this specification and to witness the functionality tests. Notify the Contracting Officer 14 days prior to starting testing operations.

3.3 ERECTION AND INSTALLATION

Perform the entire crane system erection in accordance with manufacturer's instructions under the full-time supervision of the manufacturer's representative.

3.3.1 Mechanical Alignment

Align motors, couplings, brakes, gear boxes, and drive components in accordance with manufacturer's instructions.

3.3.2 Electrical Adjustments

Adjust control system in accordance with manufacturer's instructions. Store a copy of all Control Parameter Settings (PLC, VFD). Provide the final settings and configurations data on the [Complete Schematic Wiring Diagram](#), including but not limited to, timer settings, resistor tap settings, potentiometer settings, test-point voltages, supply voltages, motor voltages, motor currents. Provide the test conditions such as ambient temperature, motor load, date performed and person performing the adjustments as part of the Operational Tests report.

3.3.3 Field Welding

Perform welding indoors, where possible. Surface of parts to be welded must be free from rust, scale, paint, grease, and other foreign matter. Minimum preheat and interpass temperatures must conform to the requirements of [AWS D14.1/D14.1M](#).

3.3.4 Field Painting

Perform painting indoors, where possible. Field painting (including touch-up) must conform to the requirements of the coating manufacturer and as specified in paragraph PAINTING SYSTEM.

3.4 FIELD QUALITY CONTROL

3.4.1 [Post-Erection Inspection](#)

After erection, the Contractor and the Contracting Officer must jointly inspect the crane bridge and hoist systems and components to verify compliance with specifications and approved submittals. Notify the Contracting Officer 14 days before the inspection. Provide for approval a report of the inspection indicating the crane is considered ready for operational tests.

Document the results of this inspection and submit the post-erection inspection report to the Contracting Officer for approval.

3.4.2 [Operational Tests](#)

Check the clearance envelope of the entire crane prior to picking or traversing any load to ensure there are no obstructions. Test the systems in service to determine that each component of the system operates as specified, is properly installed and adjusted, and is free from defects in material, manufacture, installation, and workmanship. Rectify all deficiencies disclosed by testing and retest the system or component to prove the crane is operational. The Contractor must furnish test weights, operating personnel, instruments, and other apparatus necessary to conduct field tests on each crane. Solid weights must be measured using calibrated equipment traceable to National Institute of Standards and Technology (NIST) with a minimum accuracy of plus or minus two percent.

3.4.2.1 No-Load Test

Raise and lower each hook through the full range of normal travel at rated speed for three complete cycles. Raise and lower each hook, testing other speeds of the crane. Verify proper operation of hoist limit switches. Operate the bridge and trolley in each direction the full distance between end stops and bring bumpers into contact with the end stops. Operate through the entire speed range and verify

proper brake operation. Verify correct operation of all indication and ancillary devices.

3.4.3 Test Data

Submit all crane test data recorded on appropriate test record forms suitable for retention for the life of the crane. Record operating and startup current measurements for hoist, trolley, and bridge motors using appropriate instrumentation (i.e., clamp-on ammeters). Compare recorded values with design specifications or manufacturer's recommended values; abnormal differences (i.e., greater than 10 percent from manufacturer's or design values) must be justified or appropriate adjustments performed. In addition, note, investigate, and correct any high temperatures or abnormal operation of any equipment or machinery. Record hoist, trolley, and bridge speeds during each test cycle.

3.4.4 Hook Tram Measurement

Establish a throat dimension base measurement by installing two tram points and measuring the distance between these tram points (plus or minus $1/64$ inch). Record this base dimension. Measure the distance between tram points before and after load test. An increase in the throat opening from the base measurement is cause for rejection.

3.4.5 Load Tests

- a. Perform the following tests, as specified below.
- b. Test loads used in this section are defined as the following:

Wire rope run-in load (when applicable): 25 - 50 percent of rated load.

Rated load test: 100 percent (plus 0 minus 10) of rated load.

Overload test: 125 percent (plus 0 minus 5) of rated load.

- c. Testing of cranes must be done with the use of test weights. The use of dynamometers in lieu of lifting test weights is not permitted. Each test weight for crane tests must be marked with a unique identification number and the weight in pounds. The weight marked must be the actual weight taken from the scale or other measuring device. Solid weights must be measured using calibrated equipment traceable to the National Institute of Standards and Technology (NIST), with a minimum accuracy of plus or minus two percent (i.e., indicated weight must be within plus or minus two percent of actual weight). A list of test weights, with identification numbers and weights, must be retained. The list must include the type and serial number (or other identifier) of the weighing device(s) used to weigh the test weights. Where a lifting attachment supports multiple test weights (e.g., stacked weights or multiple weights suspended from a padeye), the total capacity must be marked on the attachment. All rigging gear must meet OSHA and ASME requirements.

3.4.5.1 Wire Rope Run-In

The primary purpose of this procedure is to exercise the newly installed wire rope.

Place the load on the hook. Start at ground level and hoist up to one foot below upper limit at slow speed. Hoist down to lower limit at slow speed. Repeat hoisting and lowering of the load for approximately 10 hoisting cycles, increasing the speed for each cycle. During this test, the capacity overload lockout should not activate.

3.4.5.2 Rated Load Test

3.4.5.2.1 Hoist

- a. Static Load Test: With the trolley in the center of the bridge span, raise the test load approximately **one foot**. Hold the load for 10 minutes. Rotate the load and hook 360 degrees clockwise and

counterclockwise to check bearing operation with no binding. Observe for lowering of the load, which may indicate a malfunction of hoisting components or brakes. Verify that maximum beam and girder deflections do not exceed CMAA 74 and MHI MH27.1 design limits, as applicable.

- b. Dynamic Load Test: Raise and lower test load through the full lift range and visually observe smooth control and acceleration between points. Completely stop the machinery at least once in each direction to ensure proper brake operation.
- c. Hoist Mechanical Load Brake (or Self-locking Worm Gear): Raise test load approximately 5 feet. With the hoist controller in the neutral position, release (by hand) the holding brake. Document the method used to release the holding brake. The load brake must hold the test load. Again, with the holding brake in the released position start the test load down at slow speed and return the controller to the "off" position as the test load lowers. The load brake must stop and hold the test load.
- d. Hoist Loss of Power Test: Raise the test load to approximately 8 feet. While slowly lowering the test load, disconnect the crane's power source. Verify that the test load does not lower and that the brake is set.

3.4.5.2.2 Trolley

Operate the trolley (if space is available) the full distance of the bridge rails in each direction with a test load on the hook. Check proper functioning through the range of speeds. Verify proper brake action and stopping distance.

3.4.5.2.3 Bridge

With a test load on the hook, operate the bridge for the full length of the runway (if space is available) in one direction with the trolley at the far end of the bridge, and in the opposite direction with the trolley at the opposite end of the bridge. Use extreme caution. Check proper functioning through the range of speeds. Check for any binding of the bridge end trucks. Verify proper brake action and stopping distance. Record deficiencies. Secure from testing if deficiencies are found.

3.4.5.2.4 Trolley Loss of Power Test

Raise the test load approximately midway between the trolley and any permanent obstruction on the operating floor. Starting at a safe distance from walls or other obstructions, attain a slow speed of trolley travel. While maintaining a safe distance from obstructions, disconnect the main power source at the wall mounted safety switch (disconnect) to simulate a power failure. Verify that the trolley stops and that the brake sets properly. Measure the distance required for the trolley to stop.

3.4.5.2.5 Bridge Loss of Power Test

Raise the test load approximately midway between the trolley and any permanent obstruction on the operating floor. Starting at a safe distance from walls or other obstructions, attain a slow speed of bridge travel. While maintaining a safe distance from obstructions, disconnect the main power source at the wall mounted safety switch (disconnect) to simulate a power failure. Verify that the bridge stops and that the brake sets properly. Measure the distance required for the bridge to stop.

3.4.5.3 Overload Test

3.4.5.3.1 Hoist

Disconnect or adjust the overload limit device to allow the hoist to lift the test load. Verify proper operation of the overload limit device after it is reconnected.

- a. Static Load Test: With the trolley in the center of the bridge span, raise the test load approximately one foot. Hold the load for 10 minutes. Rotate the load and hook 360 degrees clockwise and counterclockwise to check bearing operation with no binding. Observe for lowering of the load,

which may indicate a malfunction of hoisting components or brakes.

- b. Dynamic Load Test: Raise and lower test load and visually observe smooth control. Stop the load during raising and lowering to verify that the brakes holds the load.
- c. Hoist Mechanical Load Brake (or Self-locking Worm Gear): Raise test load approximately 5 feet. With the hoist controller in the neutral position, release (by hand) the holding brake. Document the method used to release the holding brake. The load brake must hold the test load. Again, with the holding brake in the released position start the test load down at slow speed and return the controller to the "off" position as the test load lowers. The load brake must stop and hold the test load.
- d. Hoist Loss of Power Test: Raise the test load to approximately 8 feet. While slowly lowering the test load, disconnect the crane's power source. Verify that the test load does not lower and that the brake is set.

3.4.5.3.2 Trolley

Operate the trolley the full distance of the bridge rails in each direction with a test load on the hook (one cycle) through the range of speeds. Verify proper brake action.

3.4.5.3.3 Bridge

With a test load on the hook, operate the bridge for the full length of the runway in one direction with the trolley at the extreme end of the bridge, and in the opposite direction with the trolley at the opposite extreme end of the bridge (one cycle). Check proper functioning through the range of speeds. Check for any binding of the bridge end trucks and verify proper brake action. Record deficiencies. Secure from testing if deficiencies are found.

3.5 MANUFACTURER'S FIELD SERVICE REPRESENTATIVE

Furnish a qualified experienced manufacturer's field service representative to supervise the crane installation, assist in the performance of the on-site testing, and instruct personnel in the operational and maintenance features of the equipment.

3.6 OPERATION AND MAINTENANCE MANUALS

Provide two hard copies of operation and two hard copies of maintenance manuals for the equipment furnished along with an electronic copy (PDF) of each on a Compact Disc. Provide one complete set prior to performance testing and final copies upon acceptance. Provide operation manuals that detail the step-by-step procedures required for system startup, operation, and shutdown. Include the manufacturer's name, model number, parts list, and brief description of all equipment and basic operating features. List in the maintenance manuals routine maintenance procedures, including weekly, monthly, semi-annual, and annual required maintenance items, possible breakdowns and repairs, and troubleshooting guides. Also include as-built drawings, piping and equipment layout, design calculations, Control Parameter Settings and printouts of any software, and simplified wiring and control diagrams of the system as installed. Secure approval of operation and maintenance manuals prior to the field training course (as applicable).

3.7 FIELD TRAINING

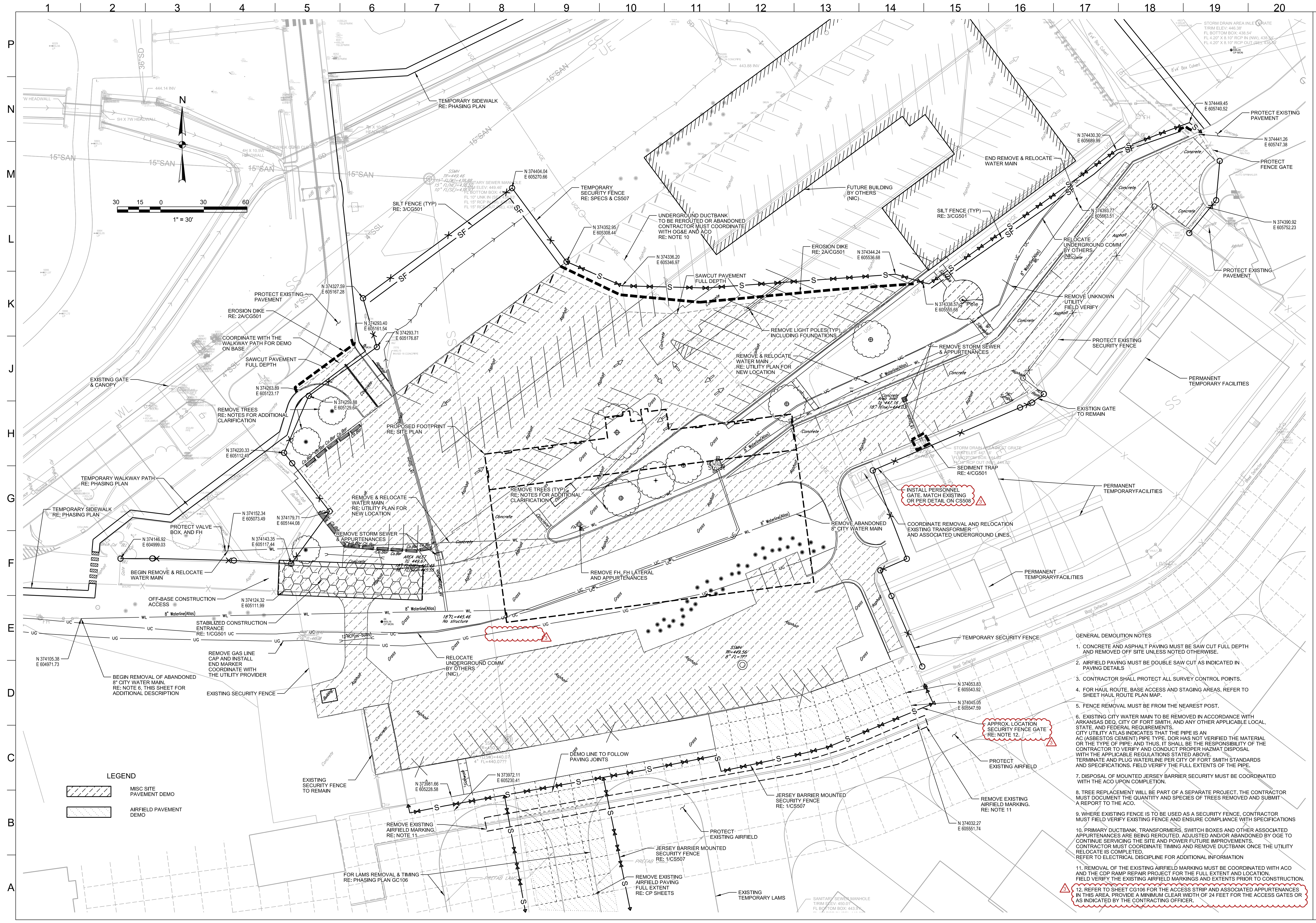
Conduct a training course for eight operating and maintenance staff and provide a copy of the training material to each participant. Provide a training period consisting of a total of four hours of normal working time and starting after the system is functionally completed but prior to final acceptance. Cover all pertinent points involved in operating, starting, stopping, and servicing the equipment, including all major elements of the Operation and Maintenance Manuals. Demonstrate in course instructions all routine maintenance operations such as lubrication, general inspection, and basic troubleshooting.

Provide a minimum four hour training session on the Variable Frequency Drives (VFDs) discussing maintenance, troubleshooting of fault codes, theory of operation, and adjustment of crane parameters. This training session will be for an audience of approximately eight people.

3.8 FINAL ACCEPTANCE

Final acceptance of crane system will not be given until Contractor has successfully completed all testing operations, corrected all material and equipment defects, made all proper operation adjustments, and removed paint or overspray on wire rope, hook, and electrical collector bars.

-- End of Section --





US Army Corps of Engineers®

DATE	DESCRIPTION
12 JAN 2026	AM 0003 - REVISED IN ACCORDANCE WITH AMENDMENT 3
3	MARK

DESIGNED BY:	ISSUE DATE:
J. ALVAREZ	5 DECEMBER 2025

DRAWN BY:	SOLICITATION NO.:
J. ALVAREZ	531870004

REVIEWED BY:	CONTRACT NO.:
J. ALVAREZ	

SUBMITTED BY:	PLOT SCALE:
A. BLANKENSHIP, P.E.	AS SHOWN

SIZE:	FILENAME:
22"x34"	EANG_512203_C_3BAYH_mdl.dgn

U.S. ARMY CORPS OF ENGINEERS
TULSA DISTRICT
2488 E. 81ST STREET
TULSA, OKLAHOMA

ENGINEERING & CONSTRUCTION DIVISION
ENGINEERING BRANCH

DEMOLITION PLAN

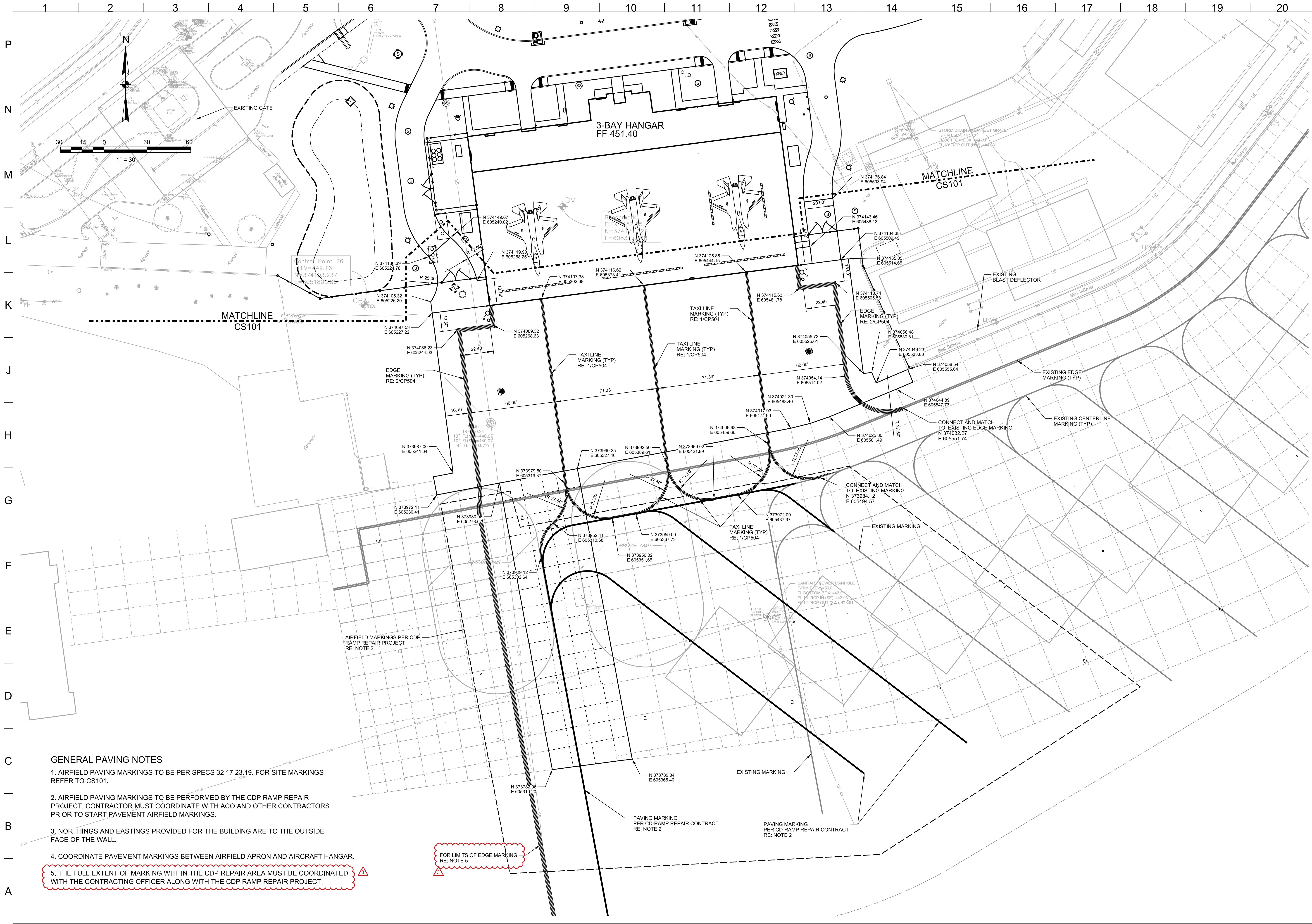
SHEET ID

CD101

GENERAL DEMOLITION NOTES

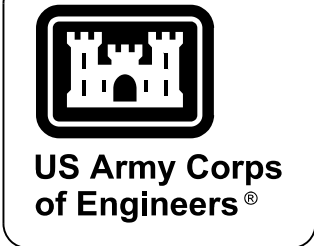
1. CONCRETE AND ASPHALT PAVING MUST BE SAW CUT FULL DEPTH AND REMOVED OFF SITE UNLESS NOTED OTHERWISE.
2. AIRFIELD PAVING MUST BE DOUBLE SAW CUT AS INDICATED IN PAVING DETAILS
3. CONTRACTOR SHALL PROTECT ALL SURVEY CONTROL POINTS.
4. FOR HAUL ROUTE, BASE ACCESS AND STAGING AREAS, REFER TO SHEET HAUL ROUTE PLAN MAP.
5. FENCE REMOVAL MUST BE FROM THE NEAREST POST.
6. EXISTING CITY WATER MAIN TO BE REMOVED IN ACCORDANCE WITH ARKANSAS DEQ, CITY OF FORT SMITH, AND ANY OTHER APPLICABLE LOCAL, STATE, AND FEDERAL REQUIREMENTS. CITY UTILITY ATLAS INDICATES THAT THE PIPE IS AN AC (ASBESTOS CEMENT) PIPE TYPE. DOR HAS NOT VERIFIED THE MATERIAL OR THE TYPE OF PIPE; AND THUS, IT SHALL BE THE RESPONSIBILITY OF THE CONTRACTOR TO VERIFY AND CONDUCT PROPER HAZMAT DISPOSAL WITH THE APPLICABLE REGULATIONS STATED ABOVE. TERMINATE AND PLUG WATERLINE PER CITY OF FORT SMITH STANDARDS AND SPECIFICATIONS. FIELD VERIFY THE FULL EXTENTS OF THE PIPE.
7. DISPOSAL OF MOUNTED JERSEY BARRIER SECURITY MUST BE COORDINATED WITH THE ACO UPON COMPLETION.
8. TREE REPLACEMENT WILL BE PART OF A SEPARATE PROJECT. THE CONTRACTOR MUST DOCUMENT THE QUANTITY AND SPECIES OF TREES REMOVED AND SUBMIT A REPORT TO THE ACO.
9. WHERE EXISTING FENCE IS TO BE USED AS A SECURITY FENCE, CONTRACTOR MUST FIELD VERIFY EXISTING FENCE AND ENSURE COMPLIANCE WITH SPECIFICATIONS
10. PRIMARY DUCTBANK, TRANSFORMERS, SWITCH BOXES AND OTHER ASSOCIATED APPURTENANCES ARE BEING REROUTED, ADJUSTED AND/OR ABANDONED BY OGE TO CONTINUE SERVICING THE SITE AND POWER FUTURE IMPROVEMENTS. CONTRACTOR MUST COORDINATE TIMING AND REMOVE DUCTBANK ONCE THE UTILITY RELOCATE IS COMPLETED. REFER TO ELECTRICAL DISCIPLINE FOR ADDITIONAL INFORMATION
11. REMOVAL OF THE EXISTING AIRFIELD MARKING MUST BE COORDINATED WITH ACO AND THE CDP RAMP REPAIR PROJECT FOR THE FULL EXTENT AND LOCATION. FIELD VERIFY THE EXISTING AIRFIELD MARKINGS AND EXTENTS PRIOR TO CONSTRUCTION.
12. REFER TO SHEET CG106 FOR THE ACCESS STRIP AND ASSOCIATED APPURTENANCES IN THIS AREA. PROVIDE A MINIMUM CLEAR WIDTH OF 24 FEET FOR THE ACCESS GATES OR AS INDICATED BY THE CONTRACTING OFFICER.

100% READY TO ADVERTISE – NOT FOR CONSTRUCTION



GENERAL PAVING NOTES

1. AIRFIELD PAVING MARKINGS TO BE PER SPECS 32 17 23.19. FOR SITE MARKINGS REFER TO CS101.
2. AIRFIELD PAVING MARKINGS TO BE PERFORMED BY THE CDP RAMP REPAIR PROJECT. CONTRACTOR MUST COORDINATE WITH ACO AND OTHER CONTRACTORS PRIOR TO START PAVEMENT AIRFIELD MARKINGS.
3. NORTHINGS AND EASTINGS PROVIDED FOR THE BUILDING ARE TO THE OUTSIDE FACE OF THE WALL.
4. COORDINATE PAVEMENT MARKINGS BETWEEN AIRFIELD APRON AND AIRCRAFT HANGAR.
5. THE FULL EXTENT OF MARKING WITHIN THE CDP REPAIR AREA MUST BE COORDINATED WITH THE CONTRACTING OFFICER ALONG WITH THE CDP RAMP REPAIR PROJECT.



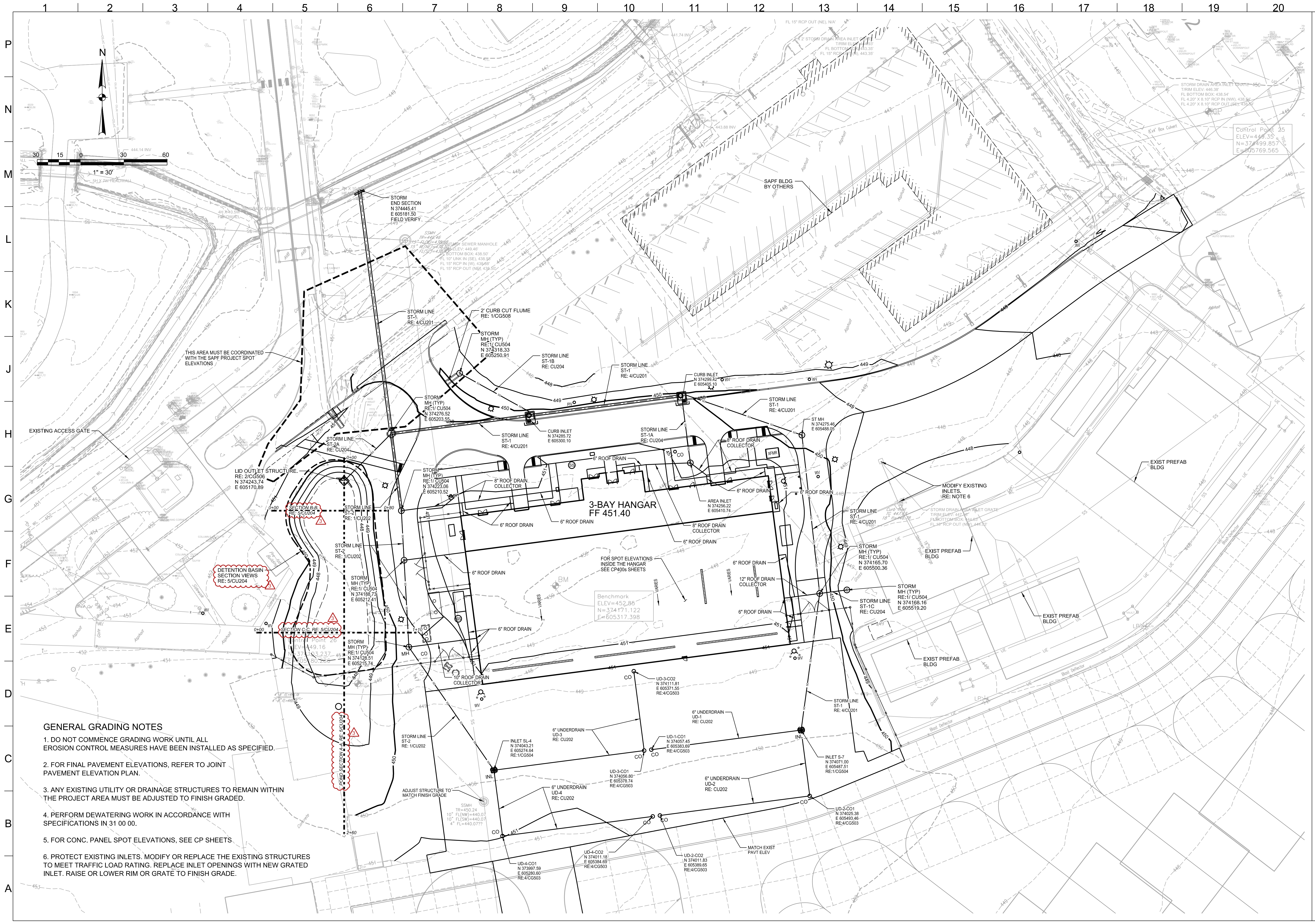
ISSUE DATE:	5 DECEMBER 2025
SOLICITATION NO.:	2488 E. 81ST STREET
CONTRACT NO.:	2488 E. 81ST STREET
CH/A:	AM 0003 - REVISED IN ACCORDANCE WITH AMENDMENT 3
DATE:	23 JAN 2026

DESIGNED BY:	J. ALVAREZ
DRAWN BY:	J. ALVAREZ
REVIEWED BY:	J. ALVAREZ
SUBMITTED BY:	A. BLANKENSHIP, P.E.
FILENAME:	EANG_512203_C_3BAYH_mdl.dgn
SIZE:	22"x34"
U.S. ARMY CORPS OF ENGINEERS	ENGINEERING & CONSTRUCTION DIVISION
TULSA DISTRICT	ENGINEERING BRANCH
2488 E. 81ST STREET	
TULSA, OKLAHOMA	

EBBING ANG, ARKANSAS	AIRFIELD PAVEMENT MARKING PLAN
F-35: 3-BAY HANGAR	
FORT SMITH, AR	
PN: 512203	

SHEET ID	CP103
----------	-------

100% READY TO ADVERTISE – NOT FOR CONSTRUCTION



GENERAL GRADING NOTES

1. DO NOT COMMENCE GRADING WORK UNTIL ALL EROSION CONTROL MEASURES HAVE BEEN INSTALLED AS SPECIFIED.
2. FOR FINAL PAVEMENT ELEVATIONS, REFER TO JOINT PAVEMENT ELEVATION PLAN.
3. ANY EXISTING UTILITY OR DRAINAGE STRUCTURES TO REMAIN WITHIN THE PROJECT AREA MUST BE ADJUSTED TO FINISH GRADED.
4. PERFORM DEWATERING WORK IN ACCORDANCE WITH SPECIFICATIONS IN 31 00 00.
5. FOR CONC. PANEL SPOT ELEVATIONS, SEE CP SHEETS
6. PROTECT EXISTING INLETS. MODIFY OR REPLACE THE EXISTING STRUCTURES TO MEET TRAFFIC LOAD RATING. REPLACE INLET OPENINGS WITH NEW GRATED INLET. RAISE OR LOWER RIM OR GRATE TO FINISH GRADE.



US Army Corps of Engineers®

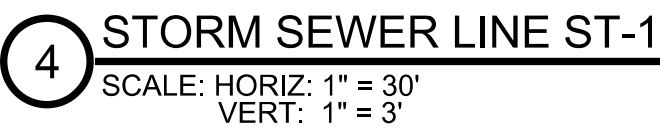
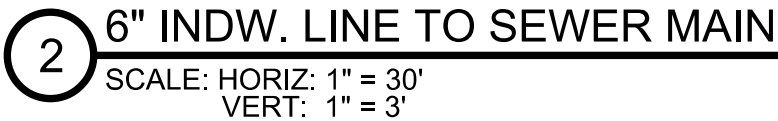
ISSUE DATE:		123 JAN 2028	
SOLICITATION NO.:		DATE	
DRAWN BY:		MARK	
REVIEWED BY:		3	
CONTRACT NO.:		AM 0003 - REVISED IN ACCORDANCE WITH AMENDMENT 3	
PLOT SCALE:		DESCRIPTION	
DESIGNED BY:	J. ALVAREZ	ISSUE DATE:	5 DECEMBER 2025
DRAWN BY:	J. ALVAREZ	SOLICITATION NO.:	2488 E. 81ST STREET
REVIEWED BY:	J. ALVAREZ	CONTRACT NO.:	TULSA, OKLAHOMA
SUBMITTED BY:	A. BLANKENSHIP, P.E.	PLOT SCALE:	AS SHOWN
SIZE:	22"x34"	FILENAME:	EANG_512203_C_3BAYH_mdl.dgn

ENGINEERING & CONSTRUCTION DIVISION
ENGINEERING BRANCH

EBBING ANG, ARKANSAS
F-35: 3-BAY HANGAR
FORT SMITH, AR
PN: 512203

GRADING PLAN

SHEET ID
CG101



100% READY TO ADVERTISE – NOT FOR CONSTRUCTION

P

N

M

L

K

J

H

G

F

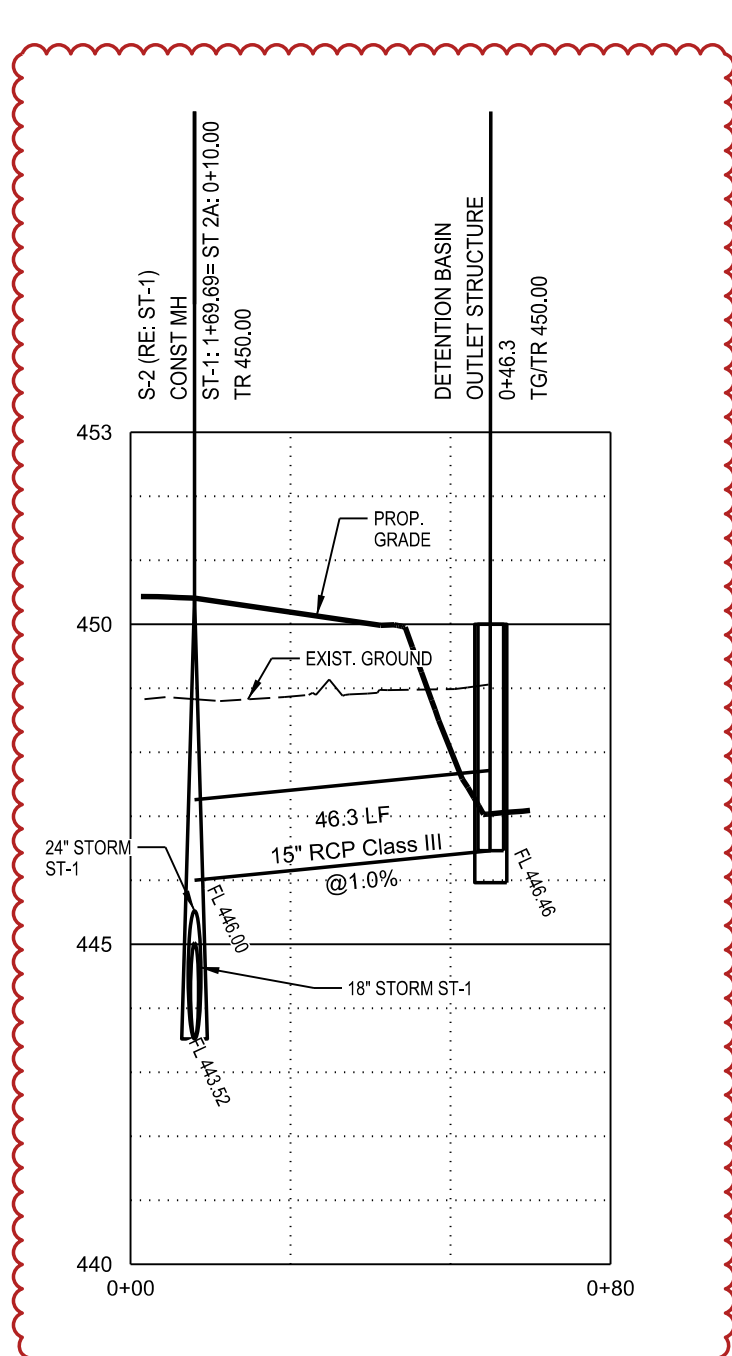
E

D

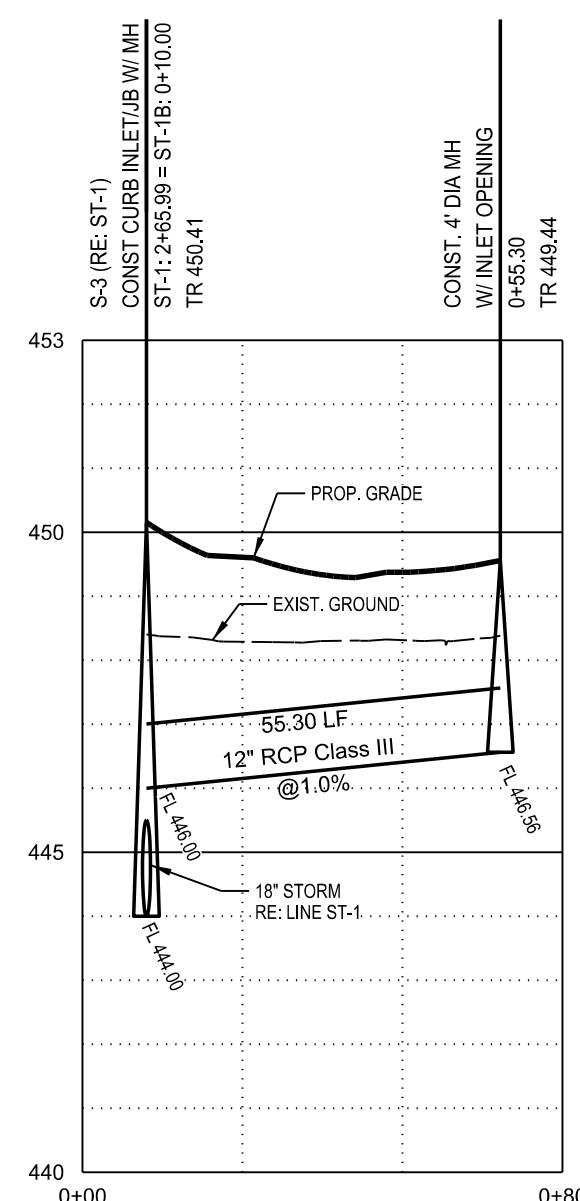
C

B

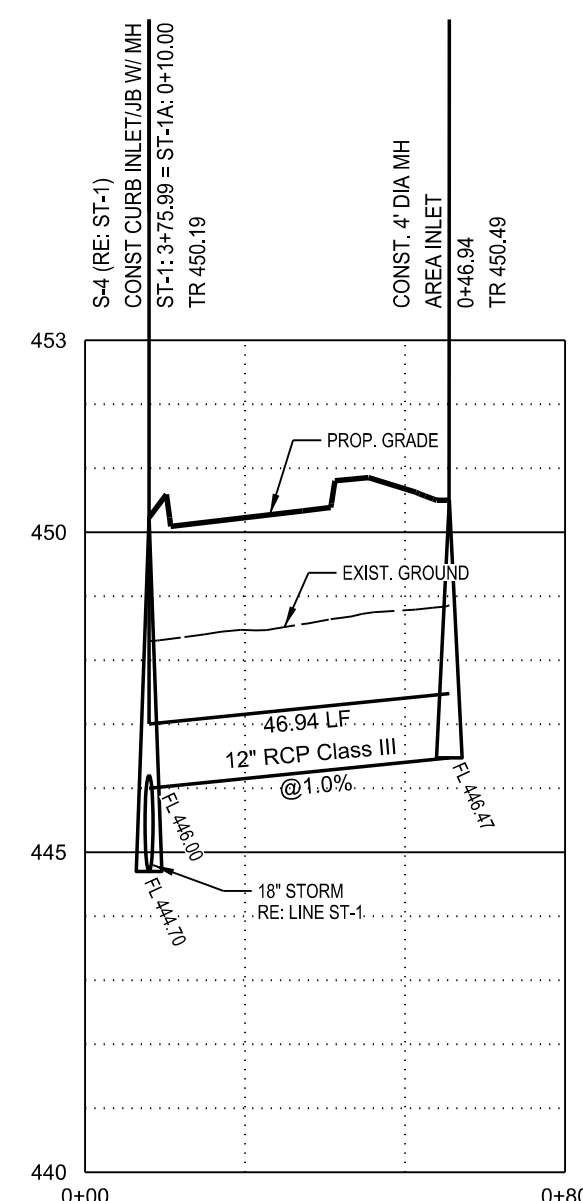
A



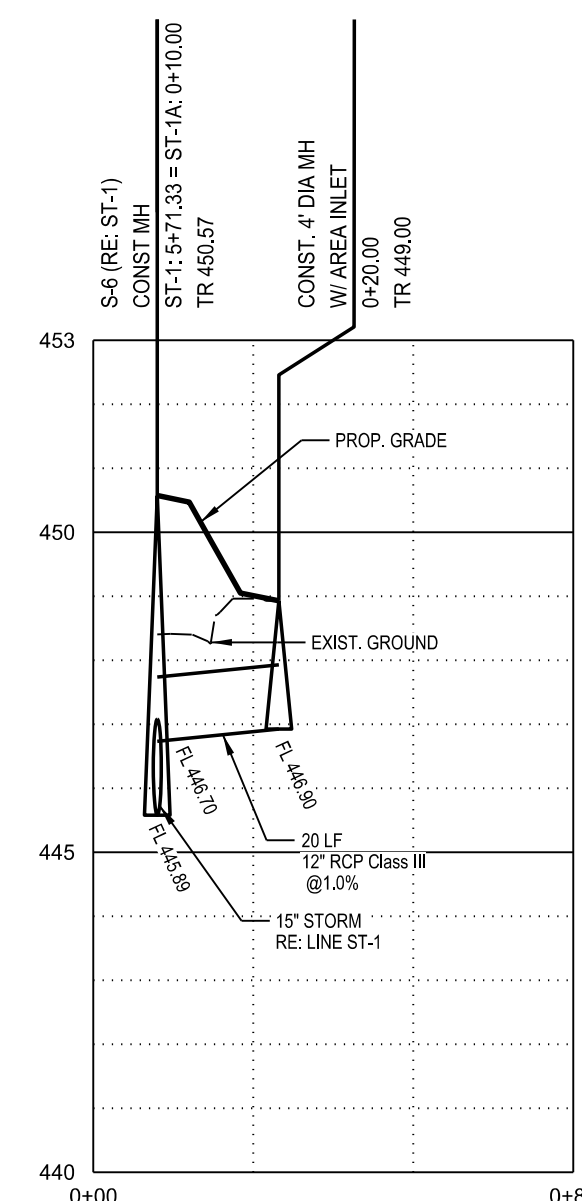
1 STORM SEWER LINE ST-2A
SCALE: HORIZ: 1" = 30'
VERT: 1" = 3'



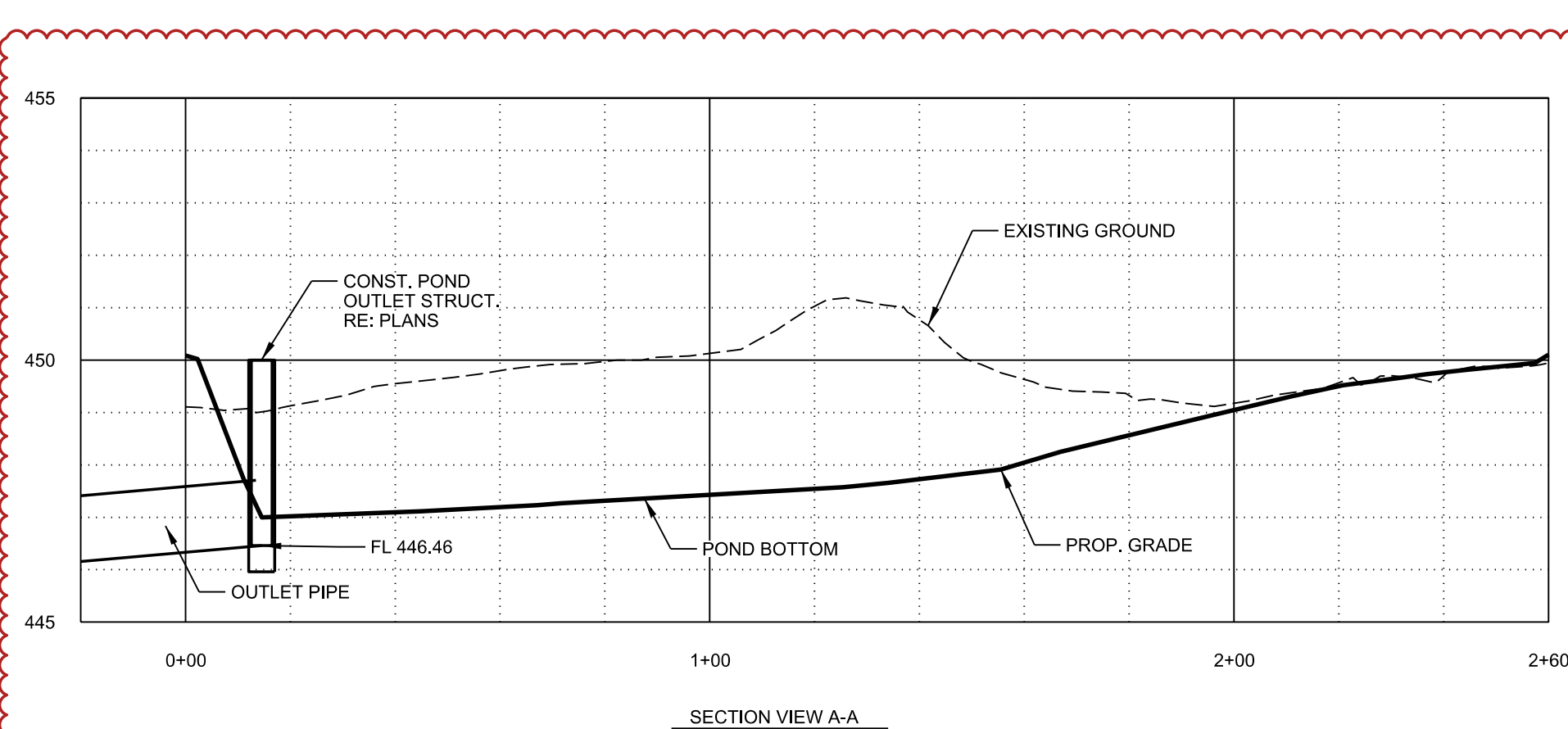
2 STORM SEWER LINE ST-1B
SCALE: HORIZ: 1" = 30'
VERT: 1" = 3'



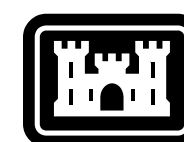
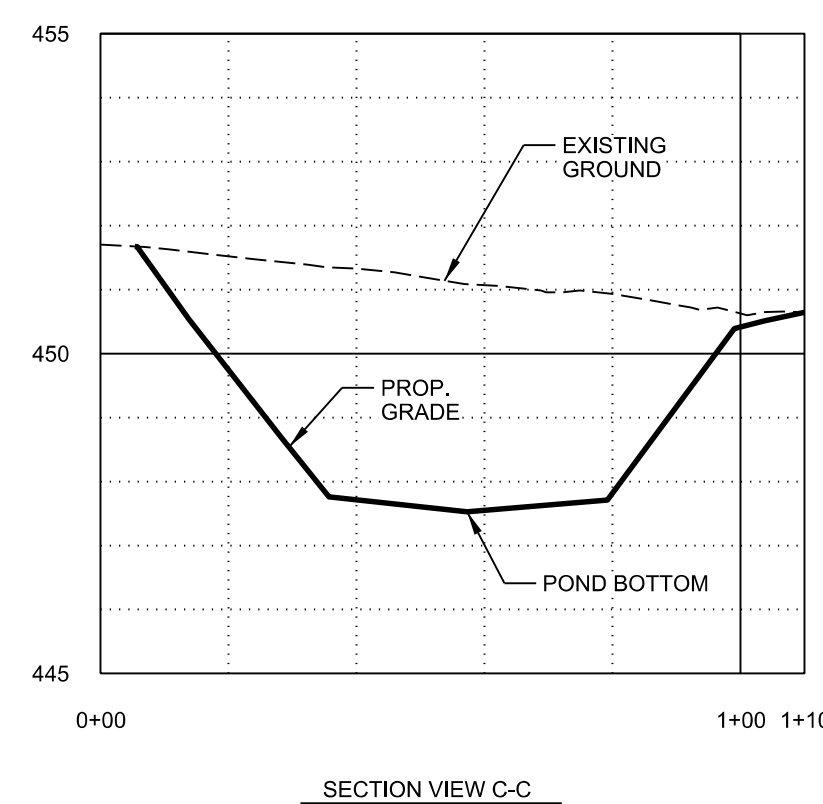
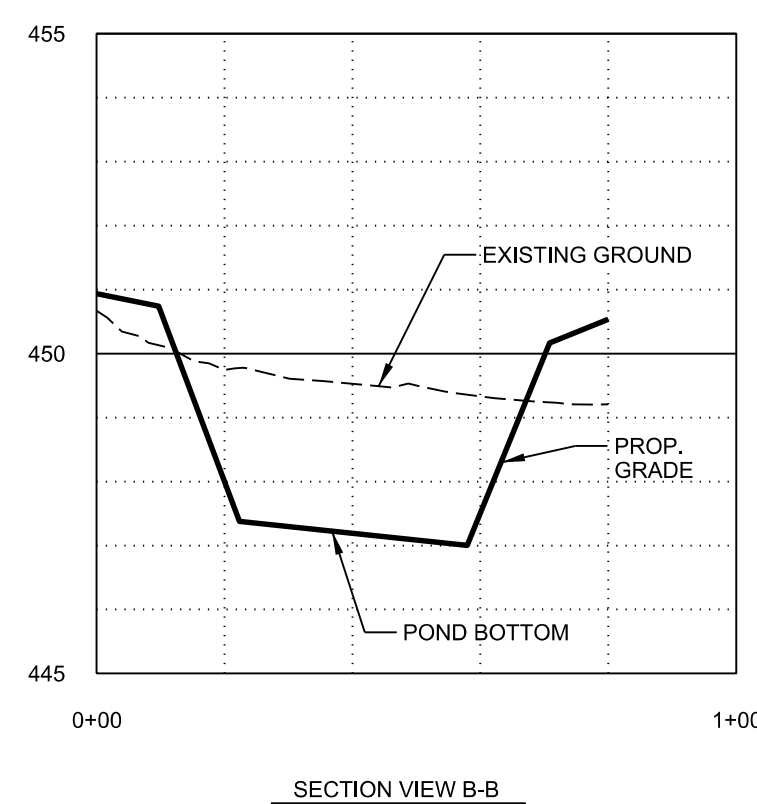
3 STORM SEWER LINE ST-1A
SCALE: HORIZ: 1" = 30'
VERT: 1" = 3'



4 STORM SEWER LINE ST-1C
SCALE: HORIZ: 1" = 30'
VERT: 1" = 3'



5 DETENTION BASIN SECTION VIEWS

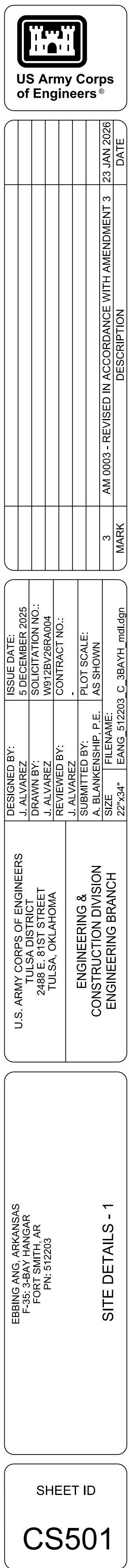
[illegible]

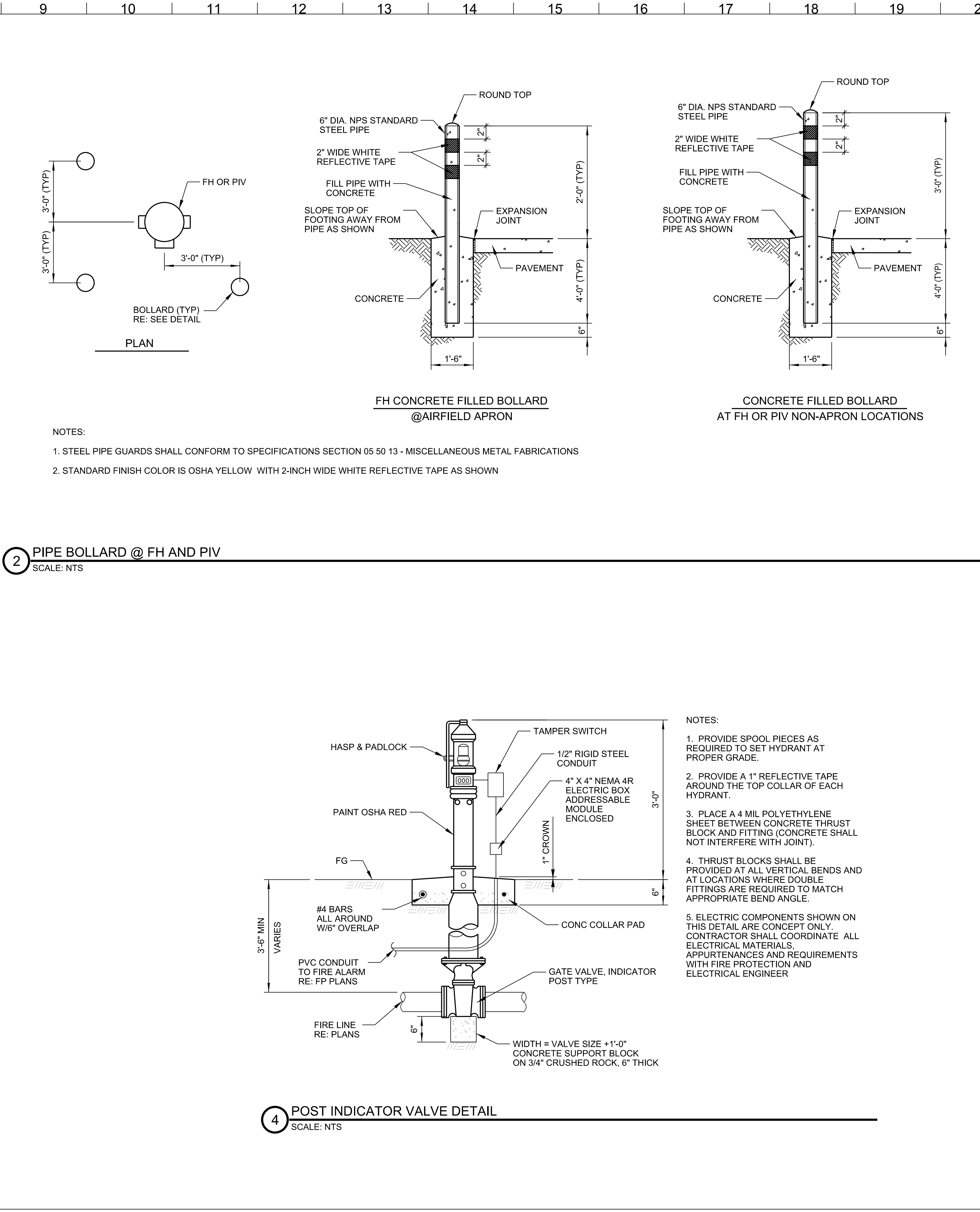
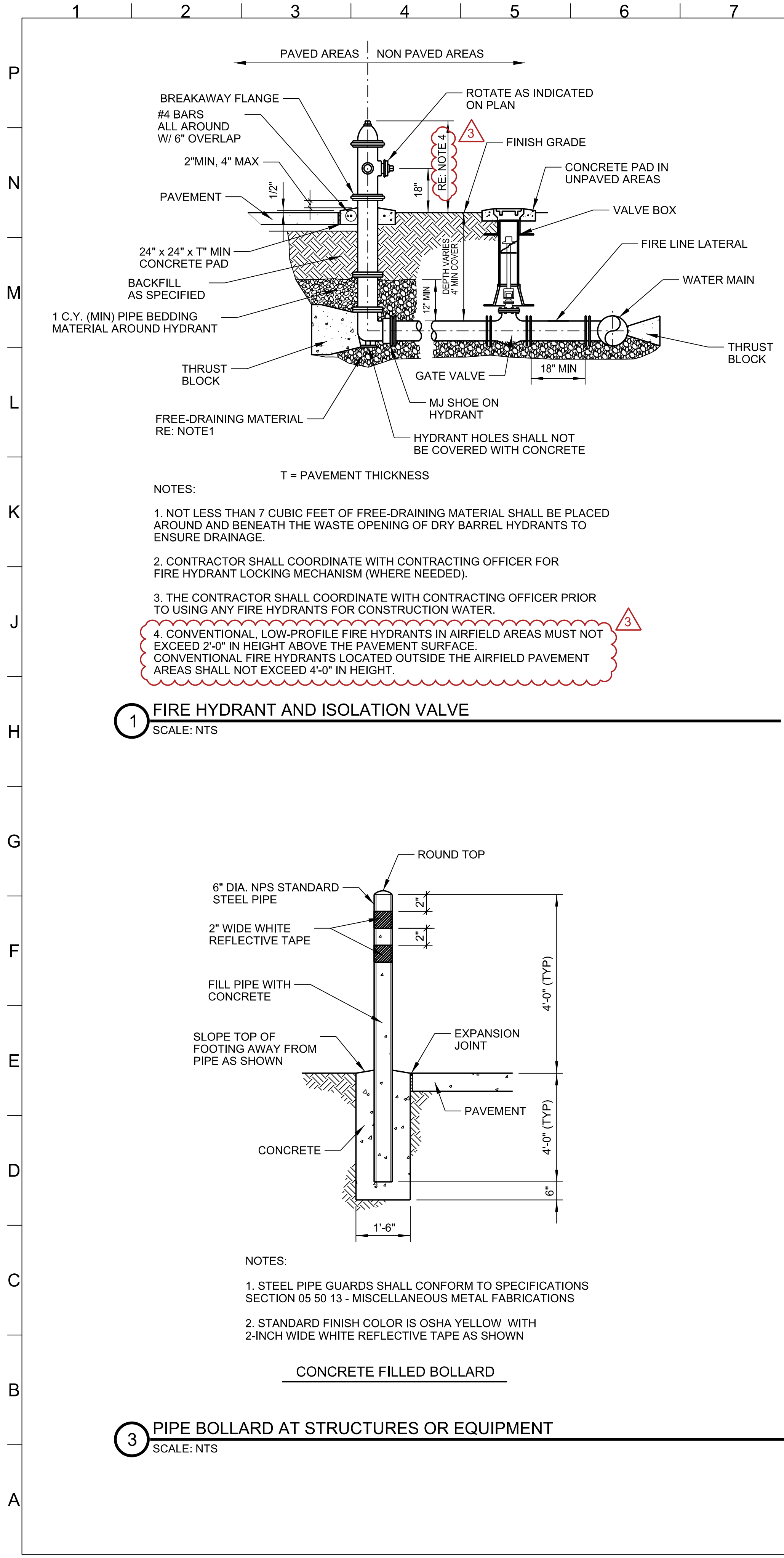
U.S. ARMY CORPS OF ENGINEERS TULSA DISTRICT 2438 E. 81ST STREET TULSA, OKLAHOMA	DESIGNED BY: J. ALVAREZ	ISSUE DATE: 5 DECEMBER 2025
	DRAWN BY: J. ALVAREZ	SOLICITATION NO.: W612B726RA004
	REVIEWED BY:	CONTRACT NO.:
	SUBMITTED BY: J. ALVAREZ	PLOT SCALE: AS SHOWN
ENGINEERING & CONSTRUCTION DIVISION ENGINEERING BRANCH	A. BLANKENSHIP, P.E. SIZE: 11x17 IN.	FILENAME: C:\Users\jlvarez\AppData\Local\Temp\1\11x17\11x17.dwg

UTILITY & STORM PROFILES

SHEET ID

CU204

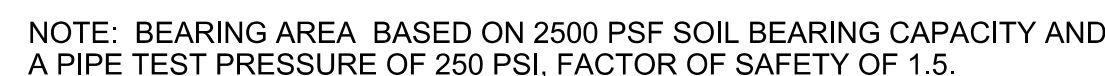




US Army Corps of Engineers®

DESIGNED BY: J. ALVAREZ	ISSUE DATE: 5 DECEMBER 2025	U.S. ARMY CORPS OF ENGINEERS TULSA DISTRICT 2488 E. 81ST STREET TULSA, OKLAHOMA	ENGINEERING & CONSTRUCTION DIVISION ENGINEERING BRANCH	UTILITY DETAILS - 1	SHEET ID CU501
DRAWN BY: J. ALVAREZ	SOLICITATION NO.: SOLICITATION NO. 04				
REVIEWED BY: J. ALVAREZ	CONTRACT NO.: -				
SUBMITTED BY: A. BLANKENSHIP, P.E.	PLOT SCALE: AS SHOWN				
FILENAME: EANG_312203_C_3BAYH_mdl.dgn	DATE: 123 JAN 2026	AM 0003 - REVISED IN ACCORDANCE WITH AMENDMENT 3	3	MARK	

100% READY TO ADVERTISE – NOT FOR CONSTRUCTION

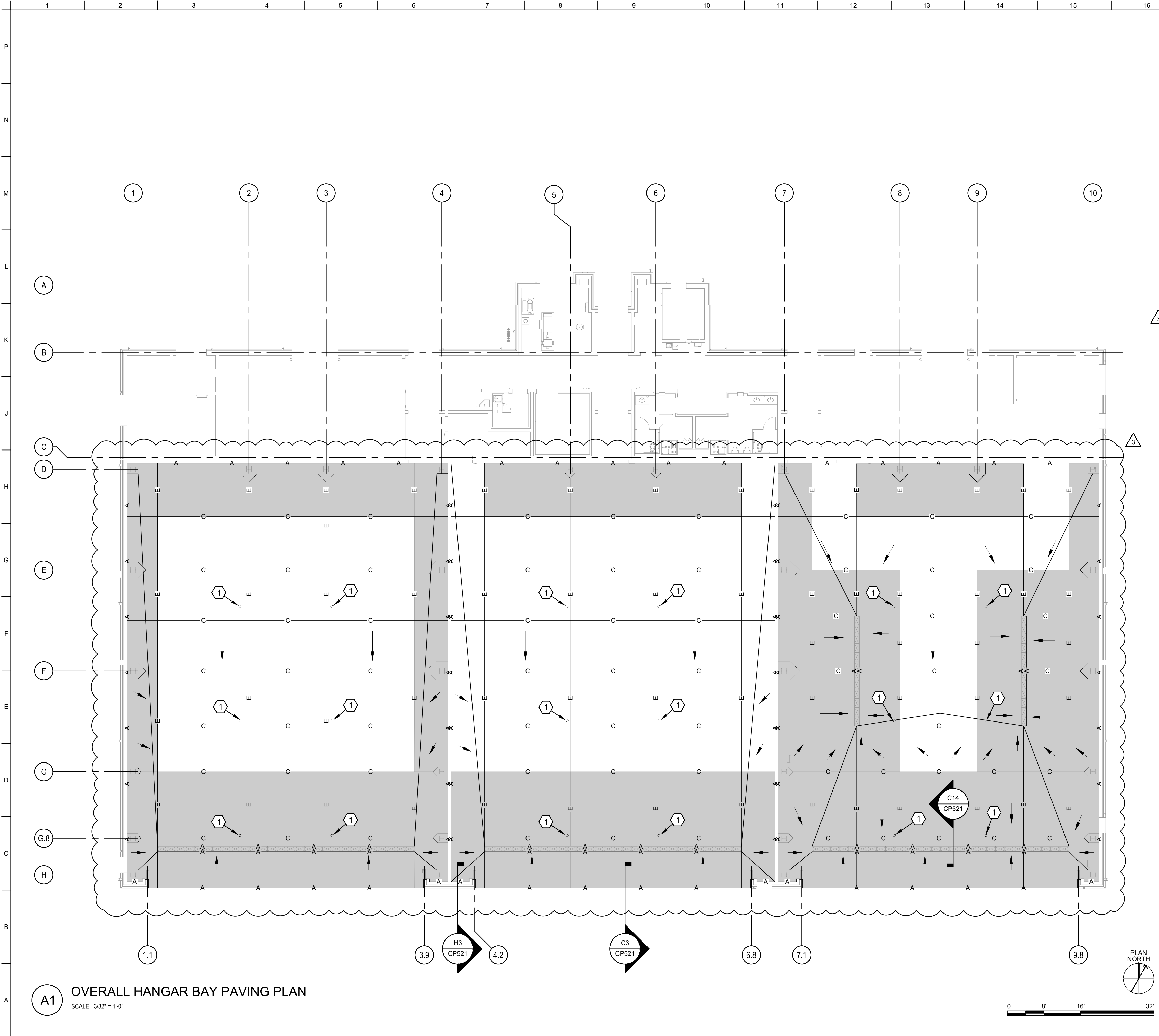


SCALE: NTS



SCALE: NTS





A1 OVERALL HANGAR BAY PAVING PLAN
SCALE: 3/32" = 1'-0"

GENERAL SHEET NOTES

- SEE PLUMBING DRAWINGS FOR TRENCH DRAIN SPECIFICATIONS.
- ALL HANGAR BAY CONCRETE TO BE 650 FLEXURAL STRENGTH AND BE IN ACCORDANCE WITH UFGS 32 13 14.13

SHEET KEY NOTES

- LOCATION OF IN-FLOOR GROUNDING RECEPTACLES. REFERENCE ELECTRICAL GROUNDING DRAWINGS.

LEGEND

- THICKENED EDGED ISOLATION JOINT
- DOWELED CONTRACTION JOINT
- DOWELED CONSTRUCTION JOINT
- INDICATES DIRECTION OF FLOOR SLOPE TOWARD DRAINS
- TRENCH DRAIN
- REINFORCED CONCRETE PAVEMENT SLAB
REF. SHEET CP501 AND CP505.



DATE	DESCRIPTION	MARK
23 JAN 2026	AM 0003 - REVISED IN ACCORDANCE WITH AMENDMENT 3	3

DESIGNED BY: W. GREEN	ISSUE DATE: 5 DECEMBER 2025
DRAWN BY: B. CASH	SOLICITATION NO: W912BV2BRAD04
CHECKED BY: J. ALVAREZ	CONTRACT NO.:
SUBMITTED BY: A. BLANKENSHIP	PROJECT NO.: 512203
SIZE: ANSI D	

U.S. ARMY CORPS OF ENGINEERS TULSA DISTRICT 2488 E 81ST ST TULSA, OK 74137	ENGINEERING & CONSTRUCTION DIVISION ENGINEERING BRANCH
---	--

SHEET ID CP420

[illegible]

U.S. ARMY CORPS OF ENGINEERS TULSA DISTRICT 2488 E. 91ST STREET TULSA, OKLAHOMA	C. HARDENW. GREEN DRAWN BY:	5 DECEMBER 2023 SOLTICATION NO.:	175 CONTRACT NO.:	175 PLOT SCALE:
	J. ALVAREZ REVIEWED BY:	W912BW2RA004 SUBMITTED BY:	175 PLANTING P.E.	175 T.S. SHOWN
	J. ALVAREZ SUBMITTED BY:	W912BW2RA004 REVIEWED BY:	175 PLANTING P.E.	175 T.S. SHOWN
	J. ALVAREZ SUBMITTED BY:	W912BW2RA004 REVIEWED BY:	175 PLANTING P.E.	175 T.S. SHOWN
	J. ALVAREZ SUBMITTED BY:	W912BW2RA004 REVIEWED BY:	175 PLANTING P.E.	175 T.S. SHOWN
ENGINEERING & CONSTRUCTION DIVISION ENGINEERING BRANCH				

EBBING ANG. ARKANSAS
F-35: 3-BAY HANGAR
FORT SMITH, AR
PN: 512203

SHEET ID

CP501



SCALE: NTS

NOTE:
1.COORDINATE SAWCUT DEPTH OF JOINT RESERVOIR WITH
SEALANT MANUFACTURER'S RECOMMENDATIONS

SCALE: NTS



SCALE: NTS



SCALE: NTS



2. CONCRETE SHALL NOT BE DRILLED UNTIL AT LEAST 72 HOURS AFTER PLACEMENT.

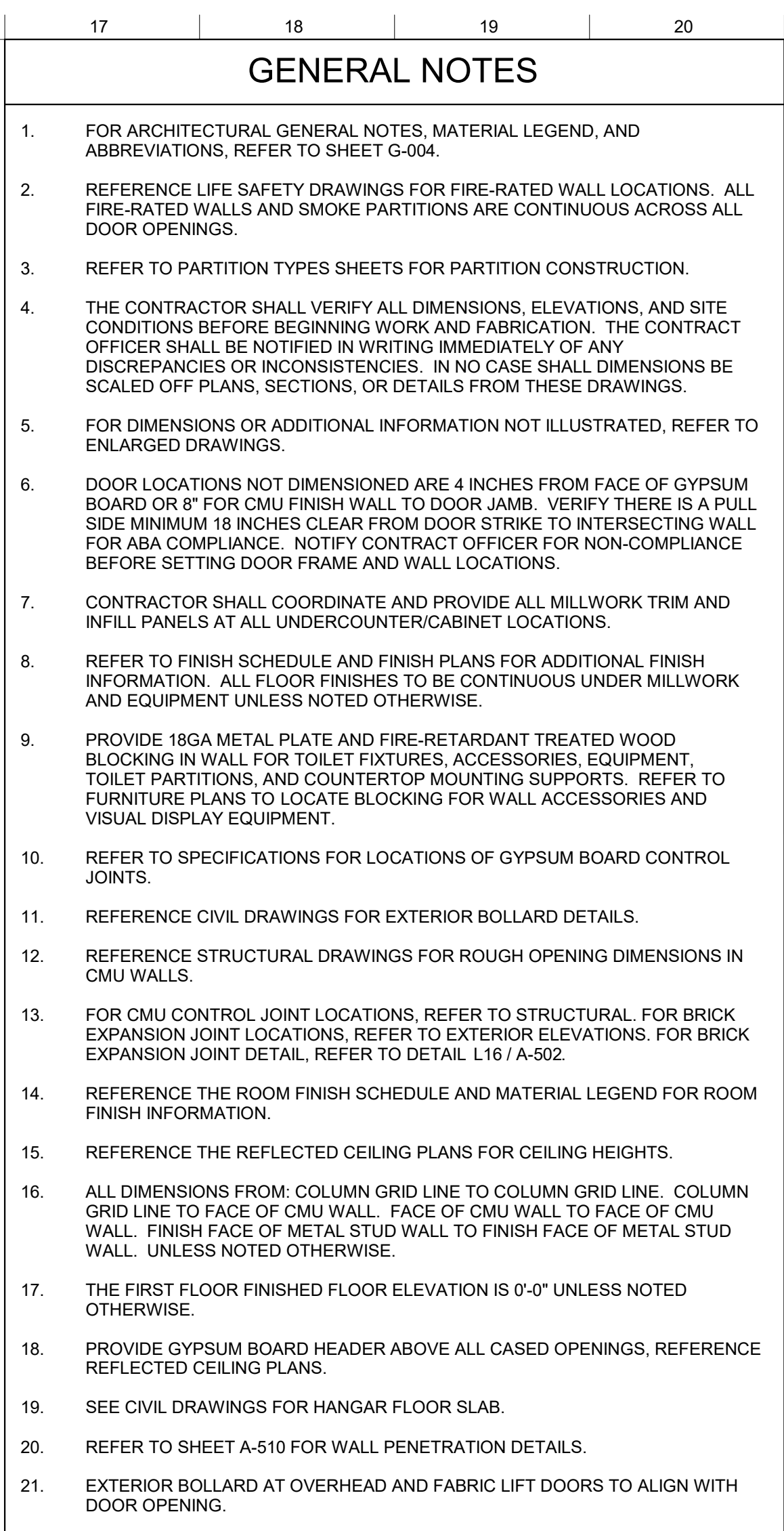
SCALE: NTS



NON-PLOT LINE TURNED OFF
FOR CLARITY ON THE LEFT SIDE
OF THE BORDER. NO DESIGN CHANGE

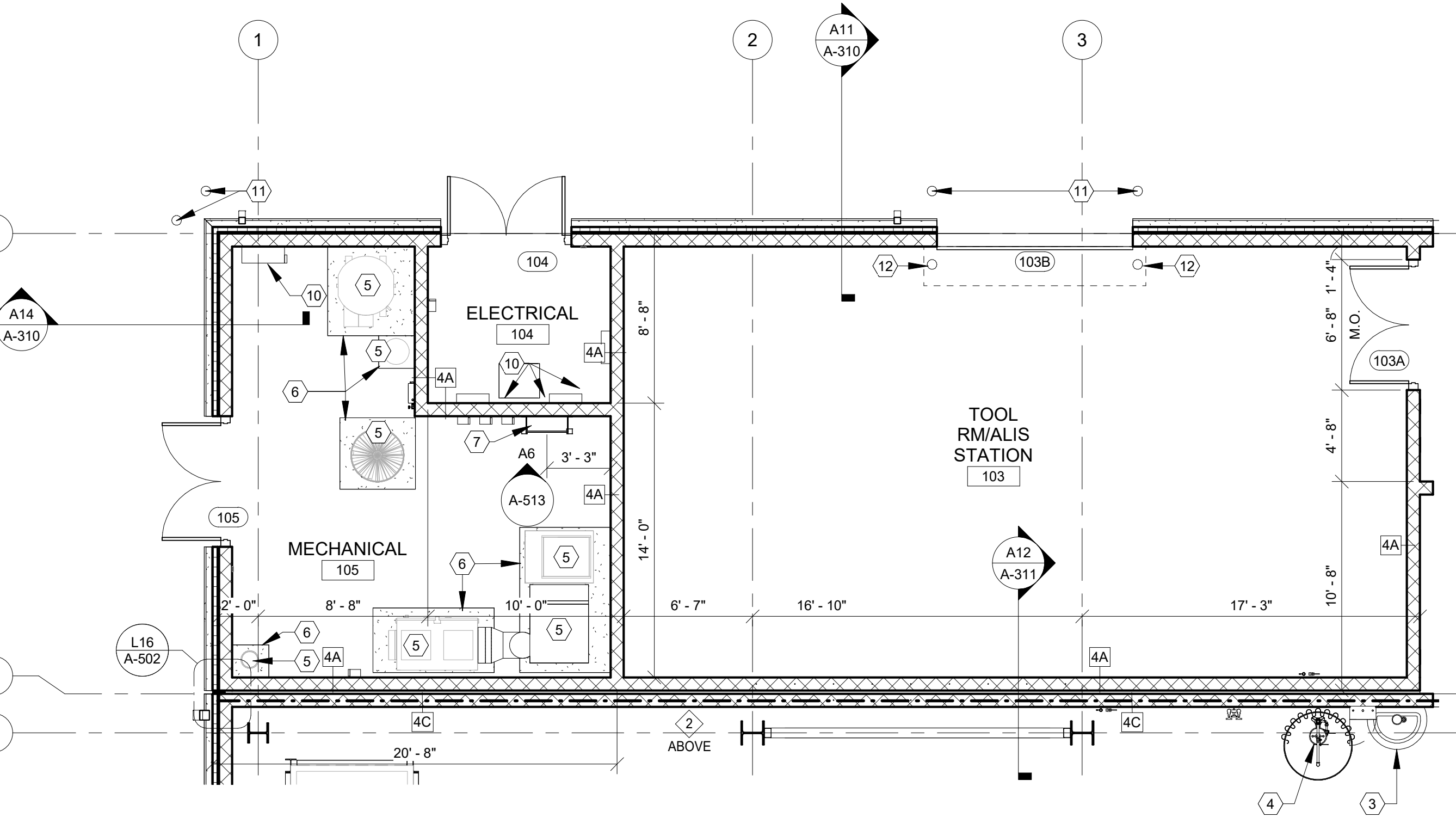
100% READY TO ADVERTISE – NOT FOR CONSTRUCTION



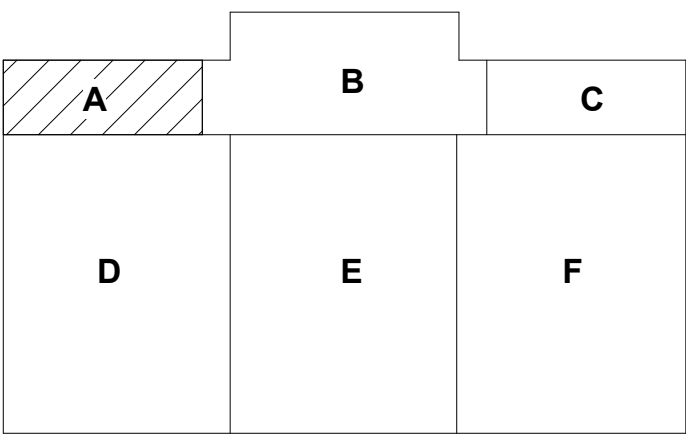
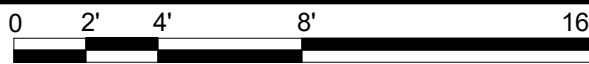


1	F-35 LIGHTNING II AIRCRAFT - TAIL IN POSITION
2	BI-FOLD VERTICAL LIFT HANGAR DOOR
3	EXTERIOR BOLLARD, REF: CIVIL

100% READY TO ADVERTISE - NOT FOR CONSTRUCTION



B2 ENLARGED FLOOR PLAN - AREA A
3/16" = 1'-0"



KEY PLAN

1-HOUR FIRE BARRIER	8" CMU WALL - REFER TO WALL TYPES AND STRUCTURAL DWGS
INDICATES DOOR NUMBER - PER DOOR SCHEDULE A-601	
INDICATES WINDOW TYPE - PER WINDOW SCHEDULE A-620	
INDICATES WALL TYPE - REFER TO WALL TYPES	

- FOR ARCHITECTURAL GENERAL NOTES, MATERIAL LEGEND, AND ABBREVIATIONS, REFER TO SHEET G-004.
- REFERENCE LIFE SAFETY DRAWINGS FOR FIRE-RATED WALL LOCATIONS. ALL FIRE-RATED WALLS AND SMOKE PARTITIONS ARE CONTINUOUS ACROSS ALL DOOR OPENINGS.
- REFER TO PARTITION TYPES SHEETS FOR PARTITION CONSTRUCTION.
- THE CONTRACTOR SHALL VERIFY ALL DIMENSIONS, ELEVATIONS, AND SITE CONDITIONS BEFORE BEGINNING WORK AND FABRICATION. THE CONTRACT OFFICER SHALL BE NOTIFIED IN WRITING IMMEDIATELY OF ANY DISCREPANCIES OR INCONSISTENCIES. IN NO CASE SHALL DIMENSIONS BE SCALED OFF PLANS, SECTIONS, OR DETAILS FROM THESE DRAWINGS.
- FOR DIMENSIONS OR ADDITIONAL INFORMATION NOT ILLUSTRATED, REFER TO ENLARGED DRAWINGS.
- DOOR LOCATIONS NOT DIMENSIONED ARE 4 INCHES FROM FACE OF GYPSUM BOARD OR CMU FINISH WALL TO DOOR JAMB. VERIFY THERE IS A PULL SIDE MINIMUM 18 INCHES CLEAR FROM DOOR STRIKE TO INTERSECTING WALL FOR ABA COMPLIANCE. NOTIFY CONTRACT OFFICER FOR NON-COMPLIANCE BEFORE SETTING DOOR FRAME AND WALL LOCATIONS.
- CONTRACTOR SHALL COORDINATE AND PROVIDE ALL MILLWORK TRIM AND INFILL PANELS AT ALL UNDERCOUNTER/CABINET LOCATIONS.
- REFER TO FINISH SCHEDULE AND FINISH PLANS FOR ADDITIONAL FINISH INFORMATION. ALL FLOOR FINISHES TO BE CONTINUOUS UNDER MILLWORK AND EQUIPMENT UNLESS NOTED OTHERWISE.
- PROVIDE 18GA METAL PLATE AND FIRE-RETARDANT TREATED BLOCKING IN WALL FOR TOILET FIXTURES, ACCESSORIES, EQUIPMENT, TOILET PARTITIONS, AND COUNTERTOP MOUNTING SUPPORTS. REFER TO FURNITURE PLANS TO LOCATE BLOCKING FOR WALL ACCESSORIES AND VISUAL DISPLAY EQUIPMENT.
- REFER TO SPECIFICATIONS FOR LOCATIONS OF GYPSUM BOARD CONTROL JOINTS.
- REFERENCE CIVIL DRAWINGS FOR EXTERIOR BOLLARD DETAILS.
- REFERENCE STRUCTURAL DRAWINGS FOR ROUGH OPENING DIMENSIONS IN CMU WALLS.
- FOR CMU CONTROL JOINT LOCATIONS, REFER TO STRUCTURAL. FOR BRICK EXPANSION JOINT LOCATIONS, REFER TO EXTERIOR ELEVATIONS. FOR BRICK EXPANSION JOINT DETAILS, REFER TO DTL L16 / A-502.
- REFERENCE THE ROOM FINISH SCHEDULE AND MATERIAL LEGEND FOR ROOM FINISH INFORMATION.
- REFERENCE THE REFLECTED CEILING PLANS FOR CEILING HEIGHTS.
- REFER TO A-101 FOR ALL EXTERIOR BUILDING DIMENSIONS, INCLUDING BUT NOT LIMITED TO: BUILDING OPENINGS, MAJOR BUILDING PROJECTIONS, AND GRID DIMENSIONS. ALL DIMENSIONS FROM COLUMN GRID LINE TO COLUMN GRID LINE. COLUMN GRID LINE TO FACE OF CMU WALL. FACE OF CMU WALL TO FACE OF CMU WALL. FINISH FACE OF METAL STUD WALL TO FINISH FACE OF METAL STUD WALL. UNLESS NOTED OTHERWISE.
- THE FIRST FLOOR FINISHED FLOOR ELEVATION IS 0'-0" UNLESS NOTED OTHERWISE.
- PROVIDE GYPSUM BOARD HEADER ABOVE ALL CASED OPENINGS, REFERENCE REFLECTED CEILING PLANS.
- SEE CIVIL DRAWINGS FOR HANGAR FLOOR SLAB.
- REFER TO SHEET A-510 FOR PENETRATION DETAILS.

ALL KEYNOTES MAY NOT BE USED ON SHEET.

①	F-35 LIGHTNING II AIRCRAFT - TAIL IN POSITION
②	VERTICAL LIFT FABRIC HANGAR DOOR
③	HANDWASH STATION, REF MECHANICAL
④	EYEWASH STATION, REF MECHANICAL
⑤	MECHANICAL EQUIPMENT, REF MECHANICAL
⑥	HOUSEKEEPING PAD, REF MECHANICAL AND STRUCTURAL
⑦	ROOF ACCESS LADDER, REF SHEET A-513
⑧	EXPANSION JOINT, REF H16 / A-502
⑨	TRENCH OR FLOOR DRAIN, REF PLUMBING
⑩	ELECTRICAL EQUIPMENT, REF ELECTRICAL
⑪	EXTERIOR BOLLARDS, REF CIVIL
⑫	INTERIOR SURFACE MOUNTED BOLLARDS, REF A1 / A-540
⑬	(2) 4' X 8' HORIZONTAL SHEETS OF 3/4" FIRE RATED PLYWOOD STACKED VERTICALLY, PAINTED. BEGIN INSTALLATION WITH BOTTOM OF LOWER SHEET ABOVE RUBBER WALL BASE. REF SPEC SECTION 27 10 00 FOR ADDITIONAL INFO
⑭	CATWALK ACCESS LADDER, REF SHEET A-516 AND A-517
⑮	KNOX BOX. FIRE DEPARTMENT TO DETERMINE FINAL LOCATION

[illegible]

ISSUE DATE:	5 DECEMBER 2025
DESIGNED BY:	C LONGACRE
DRAWN BY:	R. READER
CHECKED BY:	M. HOOPER, R.A.
SUBMITTED BY:	A. BLANKENSHIP, P.E.
PROJECT NO:	512203
SPECIFICATION NO.:	W912B/26RA004
CONTRACT NO.:	
SIZE:	A
FILE NAME:	EANG_512203_A_3BAYH_RVT2.mt

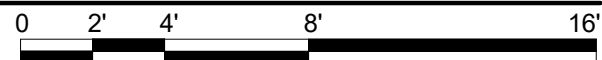
US ARMY CORPS OF ENGINEERS
TULSA DISTRICT
2488 EAST 81ST ST
TULSA, OK 74137

ENGINEERING &
CONSTRUCTION DIVISION
ENGINEERING BRANCH

EBBING ANGB - ARKANSAS
F-35: 3 BAY HANGAR
PN: 512203

SHEET ID

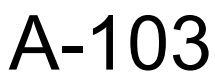
A-102



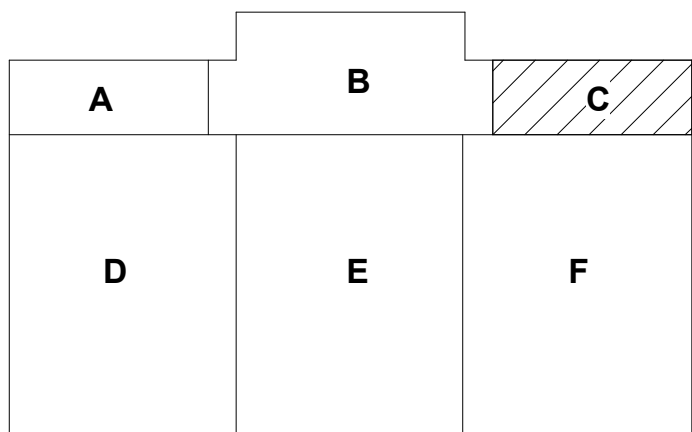
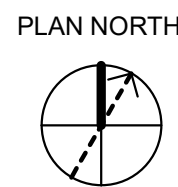
1-HOUR FIRE BARRIER	
	8" CMU WALL - REFER TO WALL TYPES AND STRUCTURAL DWGS
	INDICATES DOOR NUMBER - PER DOOR SCHEDULE A-601
	INDICATES WINDOW TYPE - PER WINDOW SCHEDULE A-620
	INDICATES WALL TYPE - REFER TO WALL TYPES

1. FOR ARCHITECTURAL GENERAL NOTES, MATERIAL LEGEND, AND ABBREVIATIONS, REFER TO SHEET G-004.
2. REFERENCE LIFE SAFETY DRAWINGS FOR FIRE-RATED WALL LOCATIONS. ALL FIRE-RATED WALLS AND SMOKE PARTITIONS ARE CONTINUOUS ACROSS ALL DOOR OPENINGS.
3. REFER TO PARTITION TYPES SHEETS FOR PARTITION CONSTRUCTION.
4. THE CONTRACTOR SHALL VERIFY ALL DIMENSIONS, ELEVATIONS, AND SITE CONDITIONS BEFORE BEGINNING WORK AND FABRICATION. THE CONTRACT OFFICER SHALL BE NOTIFIED IN WRITING IMMEDIATELY OF ANY DISCREPANCIES OR INCONSISTENCIES. IN NO CASE SHALL DIMENSIONS BE SCALED OFF PLANS, SECTIONS, OR DETAILS FROM THESE DRAWINGS.
5. FOR DIMENSIONS OR ADDITIONAL INFORMATION NOT ILLUSTRATED, REFER TO ENLARGED DRAWINGS.
6. DOOR LOCATIONS NOT DIMENSIONED ARE 4 INCHES FROM FACE OF GYPSUM BOARD OR CMU FINISH WALL TO DOOR JAMB. VERIFY THERE IS A PULL SIDE MINIMUM 18 INCHES CLEAR FROM DOOR STRIKE TO INTERSECTING WALL FOR ABA COMPLIANCE. NOTIFY CONTRACT OFFICER FOR NON-COMPLIANCE BEFORE SETTING DOOR FRAME AND WALL LOCATIONS.
7. CONTRACTOR SHALL COORDINATE AND PROVIDE ALL MILLWORK TRIM AND INFILL PANELS AT ALL UNDERCOUNTER/CABINET LOCATIONS.
8. REFER TO FINISH SCHEDULE AND FINISH PLANS FOR ADDITIONAL FINISH INFORMATION. ALL FLOOR FINISHES TO BE CONTINUOUS UNDER MILLWORK AND EQUIPMENT UNLESS NOTED OTHERWISE.
9. PROVIDE 18GA METAL PLATE AND FIRE-RETARDANT TREATED BLOCKING IN WALL FOR TOILET FIXTURES, ACCESSORIES, EQUIPMENT, TOILET PARTITIONS, AND COUNTERTOP MOUNTING SUPPORTS. REFER TO FURNITURE PLANS TO LOCATE BLOCKING FOR WALL ACCESSORIES AND VISUAL DISPLAY EQUIPMENT.
10. REFER TO SPECIFICATIONS FOR LOCATIONS OF GYPSUM BOARD CONTROL JOINTS.
11. REFERENCE CIVIL DRAWINGS FOR EXTERIOR BOLLARD DETAILS.
12. REFERENCE STRUCTURAL DRAWINGS FOR ROUGH OPENING DIMENSIONS IN CMU WALLS.
13. FOR CMU CONTROL JOINT LOCATIONS, REFER TO STRUCTURAL. FOR BRICK EXPANSION JOINT LOCATIONS, REFER TO EXTERIOR ELEVATIONS. FOR BRICK EXPANSION JOINT DETAILS, REFER TO DTL L16 / A-502.
14. REFERENCE THE ROOM FINISH SCHEDULE AND MATERIAL LEGEND FOR ROOM FINISH INFORMATION.
15. REFERENCE THE REFLECTED CEILING PLANS FOR CEILING HEIGHTS.
16. REFER TO A-101 FOR ALL EXTERIOR BUILDING DIMENSIONS, INCLUDING BUT NOT LIMITED TO: BUILDING OPENINGS, MAJOR BUILDING PROJECTIONS, AND GRID DIMENSIONS. ALL DIMENSIONS FROM: COLUMN GRID LINE TO COLUMN GRID LINE. COLUMN GRID LINE TO FACE OF CMU WALL. FACE OF CMU WALL TO FACE OF CMU WALL. FINISH FACE OF METAL STUD WALL TO FINISH FACE OF METAL STUD WALL. UNLESS NOTED OTHERWISE.
17. THE FIRST FLOOR FINISHED FLOOR ELEVATION IS 0'-0" UNLESS NOTED OTHERWISE.
18. PROVIDE GYPSUM BOARD HEADER ABOVE ALL CASSED OPENINGS, REFERENCE REFLECTED CEILING PLANS.
19. SEE CIVIL DRAWINGS FOR HANGAR FLOOR SLAB.
20. REFER TO SHEET A-510 FOR PENETRATION DETAILS.

ALL KEYNOTES MAY NOT BE USED ON SHEET.	
①	F-35 LIGHTNING II AIRCRAFT - TAIL IN POSITION
②	VERTICAL LIFT FABRIC HANGAR DOOR
③	HANDWASH STATION, REF MECHANICAL
④	EYEWASH STATION, REF MECHANICAL
⑤	MECHANICAL EQUIPMENT, REF MECHANICAL
⑥	HOUSEKEEPING PAD, REF MECHANICAL AND STRUCTURAL
⑦	ROOF ACCESS LADDER, REF SHEET A-513
⑧	EXPANSION JOINT, REF H16 / A-502
⑨	TRENCH OR FLOOR DRAIN, REF PLUMBING
⑩	ELECTRICAL EQUIPMENT, REF ELECTRICAL
⑪	EXTERIOR BOLLARDS, REF CIVIL
⑫	INTERIOR SURFACE MOUNTED BOLLARDS, REF A1 / A-540
⑬	(2) 4' X 8' HORIZONTAL SHEETS OF 3/4" FIRE RATED PLYWOOD STACKED VERTICALLY, PAINTED. BEGIN INSTALLATION WITH BOTTOM OF LOWER SHEET ABOVE RUBBER WALL BASE. REF SPEC SECTION 27 10 00 FOR ADDITIONAL INFO
⑭	CATWALK ACCESS LADDER, REF SHEET A-516 AND A-517
⑮	KNOX BOX. FIRE DEPARTMENT TO DETERMINE FINAL LOCATION



100% READY TO ADVERTISE - NOT FOR CONSTRUCTION



SHEET ID
A-104

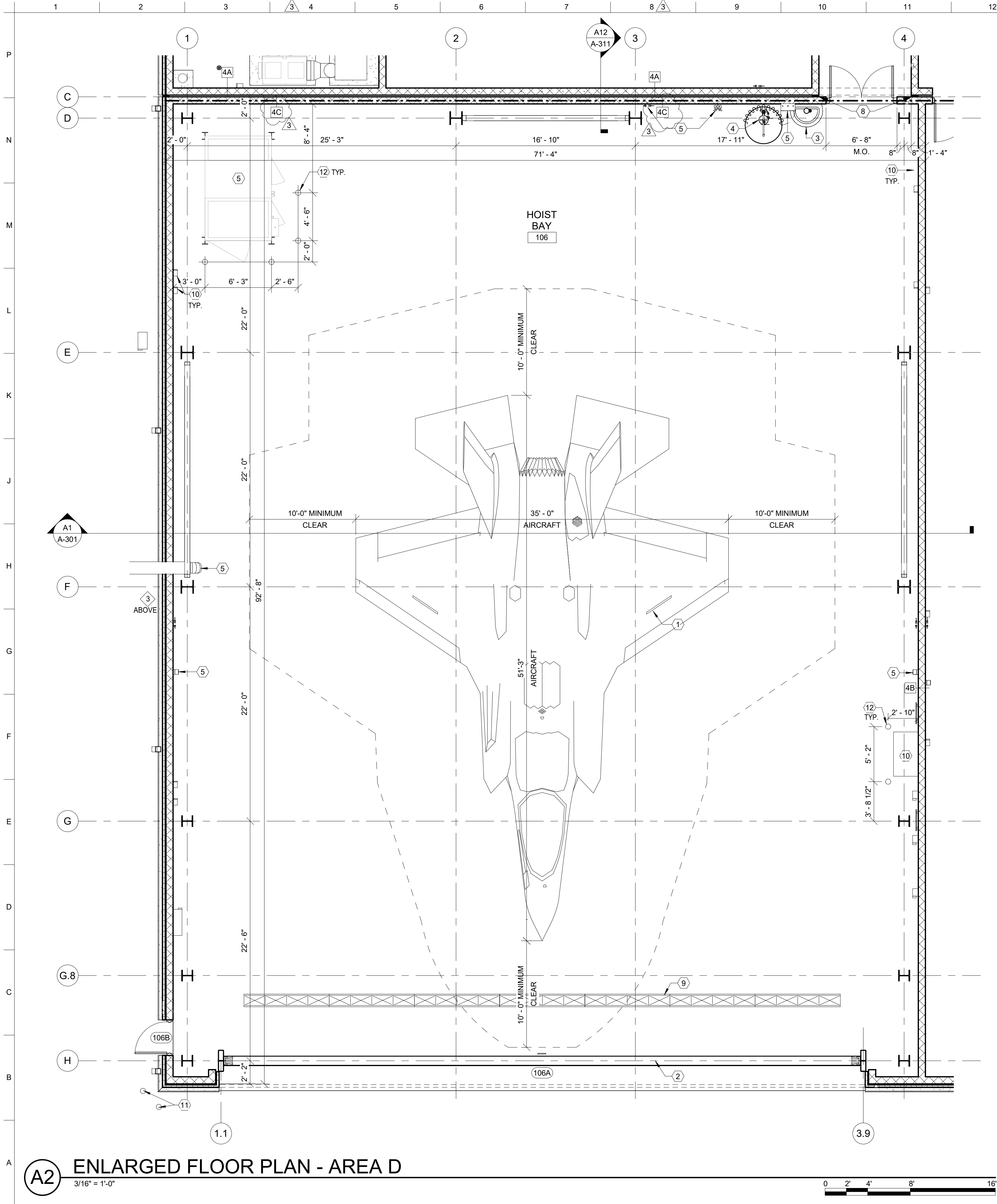
ALL KEYNOTES MAY NOT BE USED ON SHEET.	
①	F-35 LIGHTNING II AIRCRAFT - TAIL IN POSITION
②	VERTICAL LIFT FABRIC HANGAR DOOR
③	HANDWASH STATION, REF MECHANICAL
④	EYEWASH STATION, REF MECHANICAL
⑤	MECHANICAL EQUIPMENT, REF MECHANICAL
⑥	HOUSEKEEPING PAD, REF MECHANICAL AND STRUCTURAL
⑦	ROOF ACCESS LADDER, REF SHEET A-513
⑧	EXPANSION JOINT, REF H16 / A-502
⑨	TRENCH OR FLOOR DRAIN, REF PLUMBING
⑩	ELECTRICAL EQUIPMENT, REF ELECTRICAL
⑪	EXTERIOR BOLLARDS, REF CIVIL
⑫	INTERIOR SURFACE MOUNTED BOLLARDS, REF A1 / A-540
⑬	(2) 4' X 8' HORIZONTAL SHEETS OF 3/4" FIRE RATED PLYWOOD STACKED VERTICALLY, PAINTED. BEGIN INSTALLATION WITH BOTTOM OF LOWER SHEET ABOVE RUBBER WALL BASE. REF SPEC SECTION 27 10 00 FOR ADDITIONAL INFO
⑭	CATWALK ACCESS LADDER, REF SHEET A-516 AND A-517
⑮	KNOX BOX. FIRE DEPARTMENT TO DETERMINE FINAL LOCATION

US ARMY CORPS OF ENGINEERS
TULSA DISTRICT
2488 EAST 81ST ST
TULSA, OK 74137

ENGINEERING &
CONSTRUCTION DIVISION
ENGINEERING BRANCH

SHEET ID[illegible]

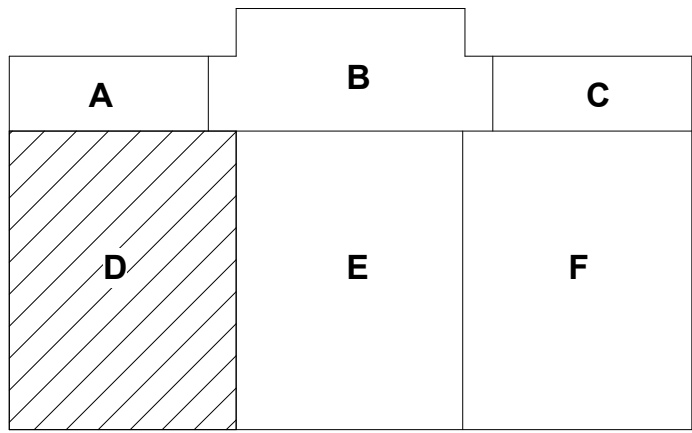
100% READY TO ADVERTISE - NOT FOR CONSTRUCTION



LEGEND	
	1-HOUR FIRE BARRIER
	8" CMU WALL - REFER TO WALL TYPES AND STRUCTURAL DWGS
	INDICATES DOOR NUMBER - PER DOOR SCHEDULE A-601
	INDICATES WINDOW TYPE - PER WINDOW SCHEDULE A-620
	INDICATES WALL TYPE - REFER TO WALL TYPES

- | GENERAL NOTES | |
|---------------|---|
| 1. | FOR ARCHITECTURAL GENERAL NOTES, MATERIAL LEGEND, AND ABBREVIATIONS, REFER TO SHEET G-004. |
| 2. | REFERENCE LIFE SAFETY DRAWINGS FOR FIRE-RATED WALL LOCATIONS. ALL FIRE-RATED WALLS AND SMOKE PARTITIONS ARE CONTINUOUS ACROSS ALL DOOR OPENINGS. |
| 3. | REFER TO PARTITION TYPES SHEETS FOR PARTITION CONSTRUCTION. |
| 4. | THE CONTRACTOR SHALL VERIFY ALL DIMENSIONS, ELEVATIONS, AND SITE CONDITIONS BEFORE BEGINNING WORK AND FABRICATION. THE CONTRACT OFFICER SHALL BE NOTIFIED IN WRITING IMMEDIATELY OF ANY DISCREPANCIES OR INCONSISTENCIES. IN NO CASE SHALL DIMENSIONS BE SCALED OFF PLANS, SECTIONS, OR DETAILS FROM THESE DRAWINGS. |
| 5. | FOR DIMENSIONS OR ADDITIONAL INFORMATION NOT ILLUSTRATED, REFER TO ENLARGED DRAWINGS. |
| 6. | DOOR LOCATIONS NOT DIMENSIONED ARE 4 INCHES FROM FACE OF GYPSUM BOARD OR CMU FINISH WALL TO DOOR JAMB. VERIFY THERE IS A PULL SIDE MINIMUM 18 INCHES CLEAR FROM DOOR STRIKE TO INTERSECTING WALL FOR ABA COMPLIANCE. NOTIFY CONTRACT OFFICER FOR NON-COMPLIANCE BEFORE SETTING DOOR FRAME AND WALL LOCATIONS. |
| 7. | CONTRACTOR SHALL COORDINATE AND PROVIDE ALL MILLWORK TRIM AND INFILL PANELS AT ALL UNDERCOUNTER/CABINET LOCATIONS. |
| 8. | REFER TO FINISH SCHEDULE AND FINISH PLANS FOR ADDITIONAL FINISH INFORMATION. ALL FLOOR FINISHES TO BE CONTINUOUS UNDER MILLWORK AND EQUIPMENT UNLESS NOTED OTHERWISE. |
| 9. | PROVIDE 18GA METAL PLATE AND FIRE-RETARDANT TREATED BLOCKING IN WALL FOR TOILET FIXTURES, ACCESSORIES, EQUIPMENT, TOILET PARTITIONS, AND COUNTERTOP MOUNTING SUPPORTS. REFER TO FURNITURE PLANS TO LOCATE BLOCKING FOR WALL ACCESSORIES AND VISUAL DISPLAY EQUIPMENT. |
| 10. | REFER TO SPECIFICATIONS FOR LOCATIONS OF GYPSUM BOARD CONTROL JOINTS. |
| 11. | REFERENCE CIVIL DRAWINGS FOR EXTERIOR BOLLARD DETAILS. |
| 12. | REFERENCE STRUCTURAL DRAWINGS FOR ROUGH OPENING DIMENSIONS IN CMU WALLS. |
| 13. | FOR CMU CONTROL JOINT LOCATIONS, REFER TO STRUCTURAL. FOR BRICK EXPANSION JOINT LOCATIONS, REFER TO EXTERIOR ELEVATIONS. FOR BRICK EXPANSION JOINT DETAILS, REFER TO DTL L16 / A-502. |
| 14. | REFERENCE THE ROOM FINISH SCHEDULE AND MATERIAL LEGEND FOR ROOM FINISH INFORMATION. |
| 15. | REFERENCE THE REFLECTED CEILING PLANS FOR CEILING HEIGHTS. |
| 16. | REFER TO A-101 FOR ALL EXTERIOR BUILDING DIMENSIONS, INCLUDING BUT NOT LIMITED TO: BUILDING OPENINGS, MAJOR BUILDING PROJECTIONS, AND GRID DIMENSIONS. ALL DIMENSIONS FROM: COLUMN GRID LINE TO COLUMN GRID LINE. COLUMN GRID LINE TO FACE OF CMU WALL. FACE OF CMU WALL TO FACE OF CMU WALL. FINISH FACE OF METAL STUD WALL TO FINISH FACE OF METAL STUD WALL. UNLESS NOTED OTHERWISE. |
| 17. | THE FIRST FLOOR FINISHED FLOOR ELEVATION IS 0'-0" UNLESS NOTED OTHERWISE. |
| 18. | PROVIDE GYPSUM BOARD HEADER ABOVE ALL CASED OPENINGS, REFERENCE REFLECTED CEILING PLANS. |
| 19. | SEE CIVIL DRAWINGS FOR HANGAR FLOOR SLAB. |
| 20. | REFER TO SHEET A-510 FOR PENETRATION DETAILS. |

KEYNOTES	
ALL KEYNOTES MAY NOT BE USED ON SHEET.	
1	F-35 LIGHTNING II AIRCRAFT - TAIL IN POSITION
2	VERTICAL LIFT FABRIC HANGAR DOOR
3	HANDWASH STATION, REF MECHANICAL
4	EYEWASH STATION, REF MECHANICAL
5	MECHANICAL EQUIPMENT, REF MECHANICAL
6	HOUSEKEEPING PAD, REF MECHANICAL AND STRUCTURAL
7	ROOF ACCESS LADDER, REF SHEET A-513
8	EXPANSION JOINT, REF H16 / A-502
9	TRENCH OR FLOOR DRAIN, REF PLUMBING
10	ELECTRICAL EQUIPMENT, REF ELECTRICAL
11	EXTERIOR BOLLARDS, REF CIVIL
12	INTERIOR SURFACE MOUNTED BOLLARDS, REF A1 / A-540
13	(2) 4' X 8' HORIZONTAL SHEETS OF 3/4" FIRE RATED PLYWOOD STACKED VERTICALLY, PAINTED. BEGIN INSTALLATION WITH BOTTOM OF LOWER SHEET ABOVE RUBBER WALL BASE. REF SPEC SECTION 27 10 00 FOR ADDITIONAL INFO
14	CATWALK ACCESS LADDER, REF SHEET A-516 AND A-517
15	KNOX BOX. FIRE DEPARTMENT TO DETERMINE FINAL LOCATION



KEY PLAN

ISSUE DATE: 5 DECEMBER 2025	DESIGNED BY: C. LONGACRE	US ARMY CORPS OF ENGINEERS TULSA DISTRICT 2466 EAST 81ST ST TULSA, OK 74137
SOLICITATION NO.: W912B123RA004	DRAWN BY: R. READER	ENGINEERING & DESIGN CONSULTING ENGINEERING BRANCH
CONTRACT NO.: M. HOOVER R.A.	CHECKED BY:	
PROJECT NO.: 512203	SUBMITTED BY: A. BLANKENSHIP P.E.	
FILE NAME: EANG_512203_A_3BAYH_RVT22.rvt	ANSI D	

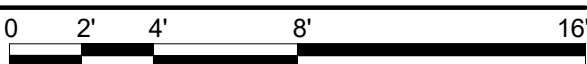
3	AM 0003 - REVISED IN ACCORDANCE WITH AMENDMENT 3	23 JAN 2026
MARK	DESCRIPTION	DATE

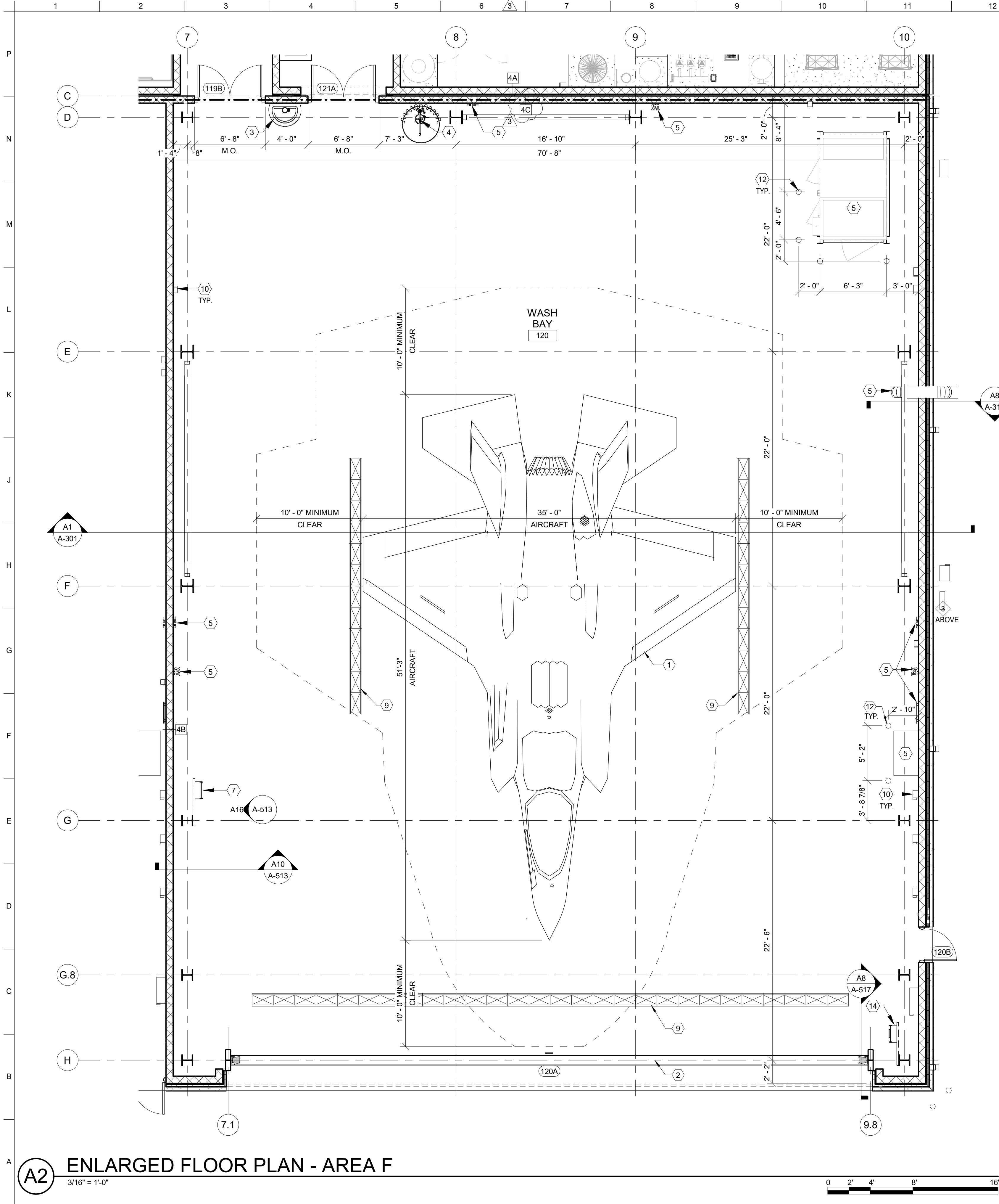
EBBING ANGB - ARKANSAS
F-35: 3 BAY HANGAR
PN: 512203

FLOOR PLAN - AREA D

SHEET ID
A-105

100% READY TO ADVERTISE - NOT FOR CONSTRUCTION



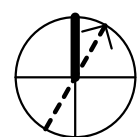


LEGEND	
	1-HOUR FIRE BARRIER
	8" CMU WALL - REFER TO WALL TYPES AND STRUCTURAL DWGS
	INDICATES DOOR NUMBER - PER DOOR SCHEDULE A-601
	INDICATES WINDOW TYPE - PER WINDOW SCHEDULE A-620
	INDICATES WALL TYPE - REFER TO WALL TYPES

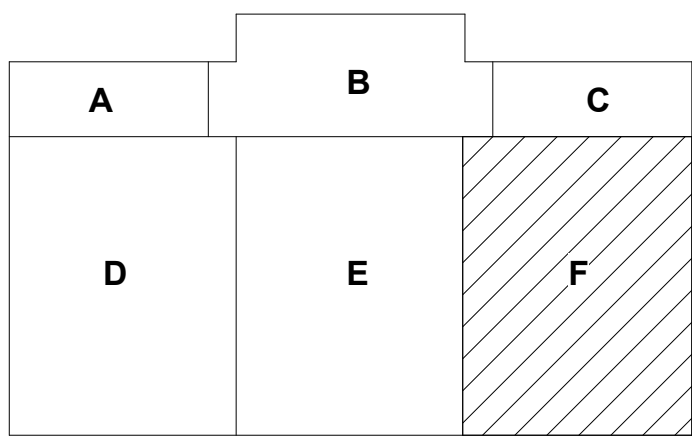
- | GENERAL NOTES | |
|---------------|---|
| 1. | FOR ARCHITECTURAL GENERAL NOTES, MATERIAL LEGEND, AND ABBREVIATIONS, REFER TO SHEET G-004. |
| 2. | REFERENCE LIFE SAFETY DRAWINGS FOR FIRE-RATED WALL LOCATIONS. ALL FIRE-RATED WALLS AND SMOKE PARTITIONS ARE CONTINUOUS ACROSS ALL DOOR OPENINGS. |
| 3. | REFER TO PARTITION TYPES SHEETS FOR PARTITION CONSTRUCTION. |
| 4. | THE CONTRACTOR SHALL VERIFY ALL DIMENSIONS, ELEVATIONS, AND SITE CONDITIONS BEFORE BEGINNING WORK AND FABRICATION. THE CONTRACT OFFICER SHALL BE NOTIFIED IN WRITING IMMEDIATELY OF ANY DISCREPANCIES OR INCONSISTENCIES. IN NO CASE SHALL DIMENSIONS BE SCALED OFF PLANS, SECTIONS, OR DETAILS FROM THESE DRAWINGS. |
| 5. | FOR DIMENSIONS OR ADDITIONAL INFORMATION NOT ILLUSTRATED, REFER TO ENLARGED DRAWINGS. |
| 6. | DOOR LOCATIONS NOT DIMENSIONED ARE 4 INCHES FROM FACE OF GYPSUM BOARD OR CMU FINISH WALL TO DOOR JAMB. VERIFY THERE IS A PULL SIDE MINIMUM 18 INCHES CLEAR FROM DOOR STRIKE TO INTERSECTING WALL FOR ABA COMPLIANCE. NOTIFY CONTRACT OFFICER FOR NON-COMPLIANCE BEFORE SETTING DOOR FRAME AND WALL LOCATIONS. |
| 7. | CONTRACTOR SHALL COORDINATE AND PROVIDE ALL MILLWORK TRIM AND INFILL PANELS AT ALL UNDERCOUNTER/CABINET LOCATIONS. |
| 8. | REFER TO FINISH SCHEDULE AND FINISH PLANS FOR ADDITIONAL FINISH INFORMATION. ALL FLOOR FINISHES TO BE CONTINUOUS UNDER MILLWORK AND EQUIPMENT UNLESS NOTED OTHERWISE. |
| 9. | PROVIDE 18GA METAL PLATE AND FIRE-RETARDANT TREATED BLOCKING IN WALL FOR TOILET FIXTURES, ACCESSORIES, EQUIPMENT, TOILET PARTITIONS, AND COUNTERTOP MOUNTING SUPPORTS. REFER TO FURNITURE PLANS TO LOCATE BLOCKING FOR WALL ACCESSORIES AND VISUAL DISPLAY EQUIPMENT. |
| 10. | REFER TO SPECIFICATIONS FOR LOCATIONS OF GYPSUM BOARD CONTROL JOINTS. |
| 11. | REFERENCE CIVIL DRAWINGS FOR EXTERIOR BOLLARD DETAILS. |
| 12. | REFERENCE STRUCTURAL DRAWINGS FOR ROUGH OPENING DIMENSIONS IN CMU WALLS. |
| 13. | FOR CMU CONTROL JOINT LOCATIONS, REFER TO STRUCTURAL. FOR BRICK EXPANSION JOINT LOCATIONS, REFER TO EXTERIOR ELEVATIONS. FOR BRICK EXPANSION JOINT DETAILS, REFER TO DTL L16 / A-502. |
| 14. | REFERENCE THE ROOM FINISH SCHEDULE AND MATERIAL LEGEND FOR ROOM FINISH INFORMATION. |
| 15. | REFERENCE THE REFLECTED CEILING PLANS FOR CEILING HEIGHTS. |
| 16. | REFER TO A-101 FOR ALL EXTERIOR BUILDING DIMENSIONS, INCLUDING BUT NOT LIMITED TO: BUILDING OPENINGS, MAJOR BUILDING PROJECTIONS, AND GRID DIMENSIONS. ALL DIMENSIONS FROM: COLUMN GRID LINE TO COLUMN GRID LINE. COLUMN GRID LINE TO FACE OF CMU WALL. FACE OF CMU WALL TO FACE OF CMU WALL. FINISH FACE OF METAL STUD WALL TO FINISH FACE OF METAL STUD WALL. UNLESS NOTED OTHERWISE. |
| 17. | THE FIRST FLOOR FINISHED FLOOR ELEVATION IS 0'-0" UNLESS NOTED OTHERWISE. |
| 18. | PROVIDE GYPSUM BOARD HEADER ABOVE ALL CASED OPENINGS, REFERENCE REFLECTED CEILING PLANS. |
| 19. | SEE CIVIL DRAWINGS FOR HANGAR FLOOR SLAB. |
| 20. | REFER TO SHEET A-510 FOR PENETRATION DETAILS. |

KEYNOTES	
ALL KEYNOTES MAY NOT BE USED ON SHEET.	
1	F-35 LIGHTNING II AIRCRAFT - TAIL IN POSITION
2	VERTICAL LIFT FABRIC HANGAR DOOR
3	HANDWASH STATION, REF MECHANICAL
4	EYEWASH STATION, REF MECHANICAL
5	MECHANICAL EQUIPMENT, REF MECHANICAL
6	HOUSEKEEPING PAD, REF MECHANICAL AND STRUCTURAL
7	ROOF ACCESS LADDER, REF SHEET A-513
8	EXPANSION JOINT, REF H16 / A-502
9	TRENCH OR FLOOR DRAIN, REF PLUMBING
10	ELECTRICAL EQUIPMENT, REF ELECTRICAL
11	EXTERIOR BOLLARDS, REF CIVIL
12	INTERIOR SURFACE MOUNTED BOLLARDS, REF A1 / A-540
13	(2) 4' X 8' HORIZONTAL SHEETS OF 3/4" FIRE RATED PLYWOOD STACKED VERTICALLY, PAINTED. BEGIN INSTALLATION WITH BOTTOM OF LOWER SHEET ABOVE RUBBER WALL BASE. REF SPEC SECTION 27 10 00 FOR ADDITIONAL INFO
14	CATWALK ACCESS LADDER, REF SHEET A-516 AND A-517
15	KNOX BOX. FIRE DEPARTMENT TO DETERMINE FINAL LOCATION

PLAN NORTH



KEY PLAN



US Army Corps of Engineers®

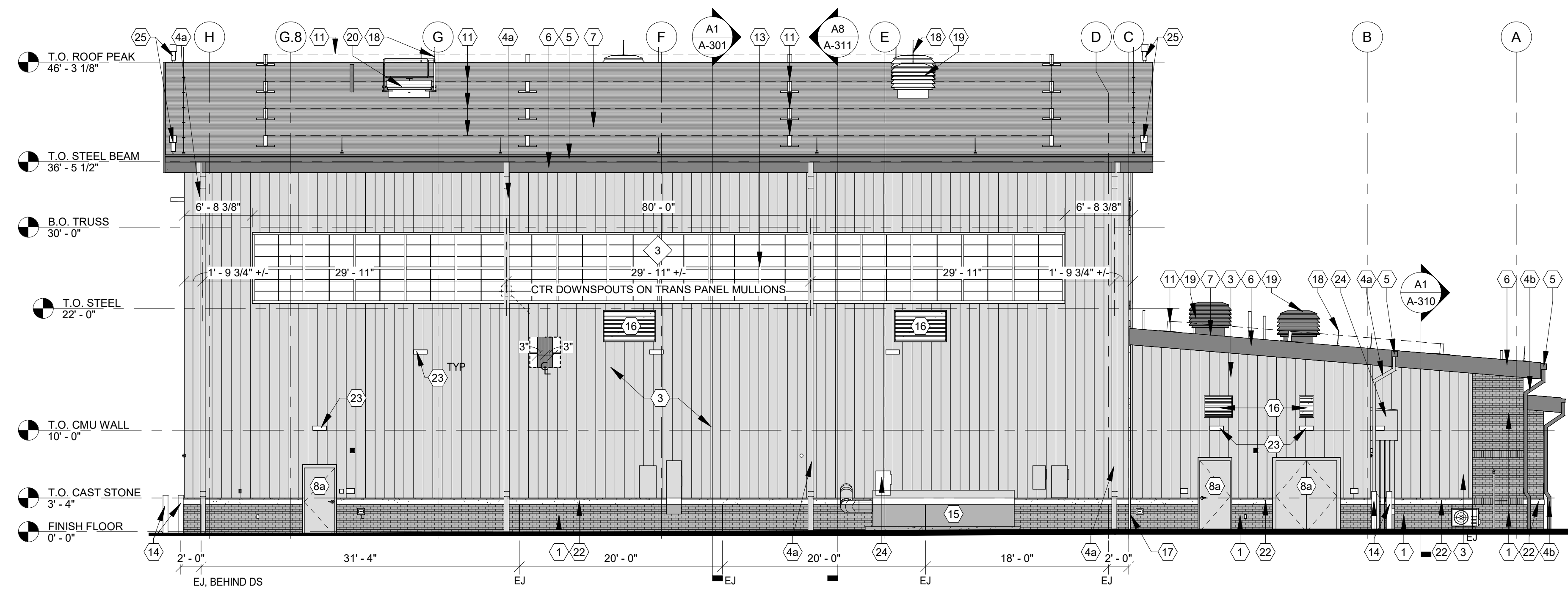
ISSUE DATE: 5 DECEMBER 2025	DESIGNED BY: C. LONGACRE	ENGINEERING & CONSTRUCTION ENGINEERING BRANCH
SOLICITATION NO.: W912BV2BR0004	DRAWN BY: R. READER	EBBING ANGB - ARKANSAS F-35: 3 BAY HANGAR PN: 512203
CONTRACT NO.:	CHECKED BY: M. HOOVER, R.A.	FLOOR PLAN - AREA F
PROJECT NO.:	SUBMITTED BY: A. BLANKENSHIP, P.E.	
FILE NAME: EANG_512203_A_38A4H_RVT22.rvt	ANSI D	
MARK	3	
DATE	23 JAN 2026	

100% READY TO ADVERTISE - NOT FOR CONSTRUCTION

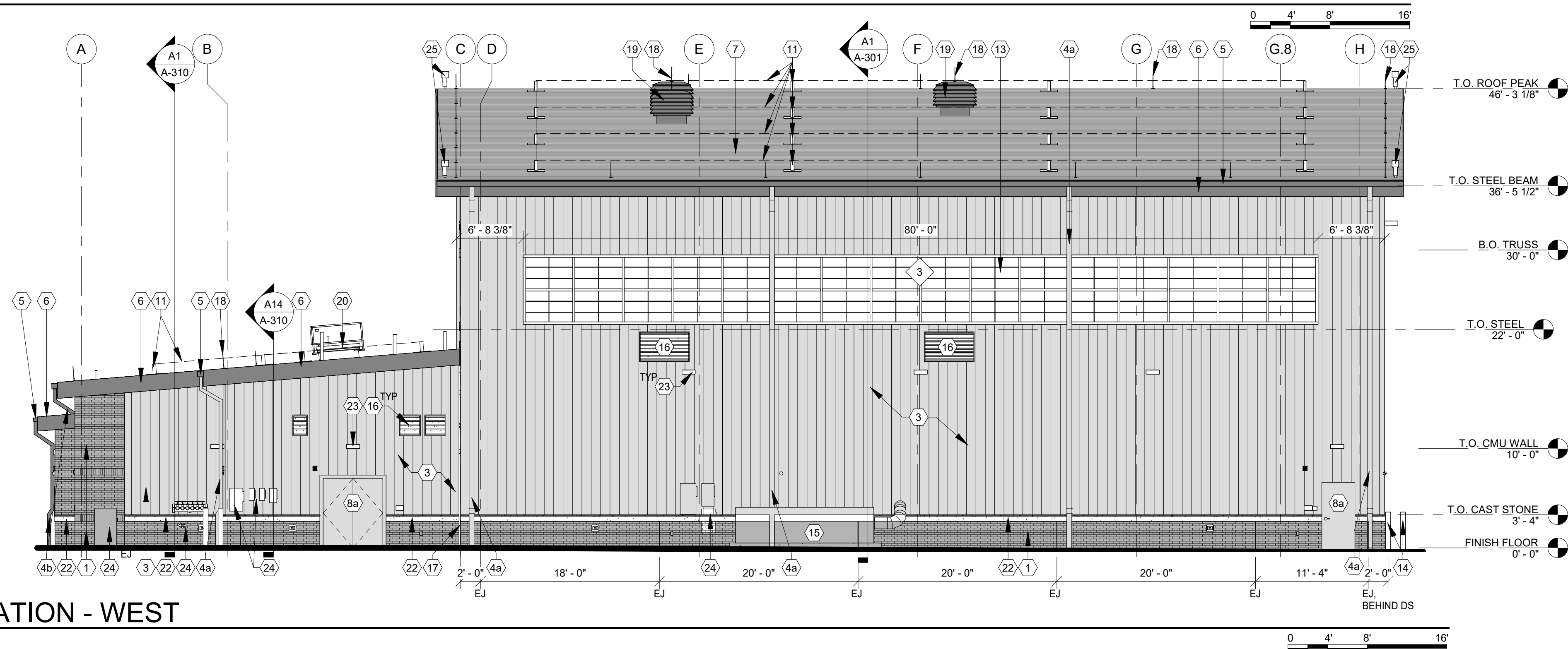
SHEET ID

A-107

		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20				
EXTERIOR FINISH LEGEND						GENERAL CONTRACTOR MUST PROVIDE SAMPLE PRODUCTS AND SAMPLE COLORS FOR APPROVAL PER SPECIFICATIONS SUBMITTAL REQUIREMENTS				KEYNOTES								GENERAL NOTES							
P	1	PRE-FINISHED STANDING SEAM METAL ROOF PANEL, AND PENETRATIONS COLOR: FED-STD-595C 30040: DARK BRONZE - HEX# 534842 OR EQUAL				9	EXTERIOR ALUMINUM DOORS AND FRAMES COLOR: ANODIZED ALUMINUM, CLEAR				ALL KEYNOTES MAY NOT BE USED ON SHEET.								1.	ALL ROOFING MATERIALS AND ACCESSORIES AND TRIM ARE TO BE PRE-FINISHED METAL.					
	2	PRE-FINISHED INSULATED METAL WALL PANEL, AND PENETRATIONS COLOR: DOVE TAIL BY METL SPAN OR EQUAL				10a 10b	EXTERIOR HOLLOW METAL DOORS AND FRAMES; (10a) MATCH DOVE TAIL (8a) (10b) MATCH DARK BRONZE - HEX# 534842 (8b)				11	MODULAR BRICK 3				15	MECHANICAL EQUIPMENT, REF. MECHANICAL				2.	ALL EXTERIOR LOUVERS SHALL BE PRE-FINISHED, COLOR WITH INSECT SCREEN, SEE LOUVER SCHEDULE ON MECHANICAL DWGS.			
	3	PRE-FINISHED STANDING SEAM METAL ROOF PANEL, AND PENETRATIONS COLOR: DOVE TAIL BY METL SPAN OR EQUAL				10a 10b	EXTERIOR HOLLOW METAL DOORS AND FRAMES; (10a) MATCH DOVE TAIL (8a) (10b) MATCH DARK BRONZE - HEX# 534842 (8b)				12	MODULAR BRICK SOLDIER COURSE 4				16	MECHANICAL LOUVER, REF. MECHANICAL FOR LOUVER SCHEDULES 7a 7b				3.	ALL EXTERIOR STEEL (UNDERSIDE OF EVES, GATES, HANDRAILS, ETC.) TO BE SHOP PRIMED AND FIELD PAINTED TO MATCH EXTERIOR COLOR.			
N	3	EXTERIOR BRICK VENEER (PRIMARY FACADE) COLOR: FLYING RAZORBACK BLEND BY ACME BRICK OR EQUAL				11	OVERHEAD COILING DOORS AND FRAMES COLOR: MATCH DOVE TAIL BY METL SPAN OR EQUAL				13	METAL WALL PANELS, INSULATED 2				17	WALL EXPANSION JOINT, REF. DETAIL F15 / A-502				4.	PROVIDE EXPANSION JOINTS IN BRICK VENEER AT 24'-0" O.C. MAX., DENOTED BY 'EJ'. SEE ARCHITECTURAL ELEVATIONS FOR LOCATIONS. REF L16 / A-502			
	4	EXTERIOR BRICK VENEER, SOLDIER COURSE (ACCENT) COLOR: FLYING RAZORBACK BLEND BY ACME BRICK OR EQUAL				12	EXTERIOR CONCRETE FILLED BOLLARDS. REF CIVIL PLANS COLOR: OSHA YELLOW WITH 2 STRIPS OF 2" WIDE WITH REFLECTIVE TAPE, 2" FROM TOP AND 2" BETWEEN THEM				14	PRE-FINISHED METAL DOWNSPOUTS (DS), REF. ROOF PLAN FOR SIZES 7a 7b				18	LIGHTNING PROTECTION, REF. ELECTRICAL				5.	METAL DOWNSPOUTS AT METAL PANEL WALLS SHALL BE PRE-FINISHED. COLOR TO MATCH METAL WALL PANEL.			
	5	CAST STONE COLOR: DARK BUFF BY DFW CAST STONE OR EQUAL				13	ROOF ACCESS LADDER COLOR: OSHA YELLOW				15	CONTINUOUS PRE-FINISHED METAL GUTTERS, REF. ROOF PLAN FOR SIZES 8				19	MECHANICAL ROOF VENT, REF. MECHANICAL 15				6.	INSTALL STANDING SEAM METAL ROOFING PER MANUFACTURER'S SPECIFICATIONS.			
M	6	TRANSLUCENT FIBERGLASS SANDWICH PANEL ASSEMBLIES COLOR: ALUMINUM PER AAMA 2605				14	VERTICAL LIFT FABRIC DOOR COLOR: WHITE				16	PRE-FINISHED METAL FASCIA AND SOFFITS, REF. DETAILS FOR SIZES 8				20	ROOF ACCESS HATCH 15				7.	SEE CIVIL PLANS FOR SITE COMPONENTS.			
	7a 7b	METAL DOWNSPOUTS AND LOUVERS (7a) MATCH DOVE TAIL (4a) (7b) MATCH DARK BRONZE - HEX# 534842 (4b)				15	ROOF ELEMENTS COLOR: FINISH TO MATCH ROOF, DARK BRONZE - HEX# 534842 OR EQUAL				17	STANDING SEAM METAL ROOF PANELS 1				21	CAST STONE LINTEL 5				8.	REFERENCE FIRE PROTECTION PLANS FOR ALL WORK ASSOCIATED TO FIRE PROTECTION SYSTEM DESIGN, INCLUDING THE REQUIRED EQUIPMENT TO BE INSTALLED ON THE EXTERIOR ELEVATIONS. COORDINATE WITH PLUMBING DRAWINGS ACCORDINGLY.			
	8	METAL COPING, FASCIA, AND GUTTERS COLOR: MATCH ROOF, DARK BRONZE - HEX# 534842 OR EQUAL				15	ROOF ELEMENTS COLOR: FINISH TO MATCH ROOF, DARK BRONZE - HEX# 534842 OR EQUAL				18	HOLLOW METAL DOOR, REF. DOOR SCHEDULE 10a 10b				22	CAST STONE WATER TABLE 5				9.	REFERENCE ELECTRICAL PLANS FOR ALL EXTERIOR LIGHT FIXTURES.			
											19	VERTICAL LIFT BIFOLD DOOR, REF. DOOR SCHEDULE 14				23	WALL PACK LIGHTING, REF. ELECTRICAL								
											20	INSULATED OVERHEAD COILING DOOR 11				24	ELECTRICAL EQUIPMENT, REF. ELECTRICAL								
											21	ROOF FALL PROTECTION, FOR LOCATIONS REF. SHEET A-110				25	OBSTRUCTION LIGHTING, REF. ELECTRICAL								
											22	INSULATED ALUMINUM STOREFRONT ASSEMBLY 9													
											23	TRANSLUCENT FIBERGLASS SANDWICH PANEL ASSEMBLIES, REF. SHEET A-620 6													
											24	6" CONCRETE FILLED STEEL BOLLARD, REF. CIVIL DETAILS 12													



(F1) EXTERIOR ELEVATION - EAST
1/8" = 1'-0"



A1 EXTERIOR ELEVATION - WEST
1/8" = 1'-0"



**US Army Corps
of Engineers ®**

[illegible]

ISSUE DATE:	5 DECEMBER 2025
SOLICITATION NO.:	W912BV26RA004
CONTRACT NO.:	
PROJECT NO:	512203
DESIGNED BY:	C. LONGACRE
DRAWN BY:	R. READER
CHECKED BY:	M. HOOPER, R.A.
SUBMITTED BY:	A. BLANKENSHIP, P.E.
SIZE:	FILE NAME:
ANS/D	EANG 512203 A 38AYH RV722.rvt

US ARMY CORPS OF ENGINEERS
TULSA DISTRICT
2488 EAST 81ST ST
TULSA, OK 74137

ENGINEERING &
CONSTRUCTION DIVISION
ENGINEERING BRANCH

EXTERIOR ELEVATIONS

F-35: 3 BAY HANGAR
PN: 512203

SHEET ID

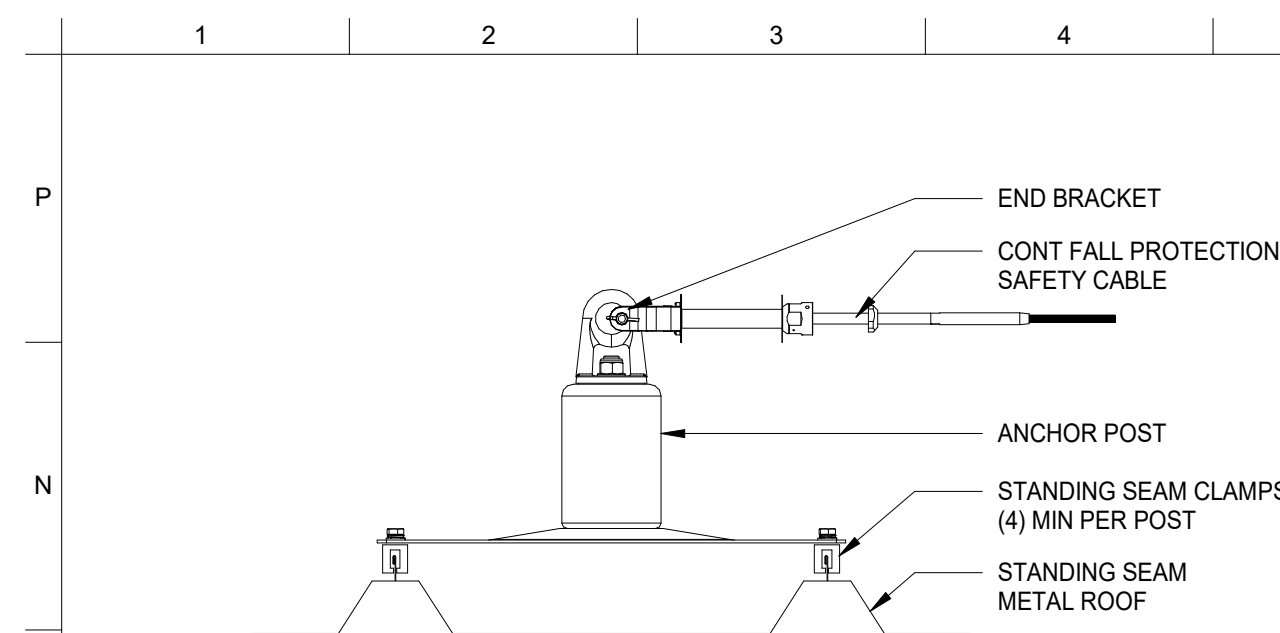
A-202

100% READY TO ADVERTISE - NOT FOR CONSTRUCTION

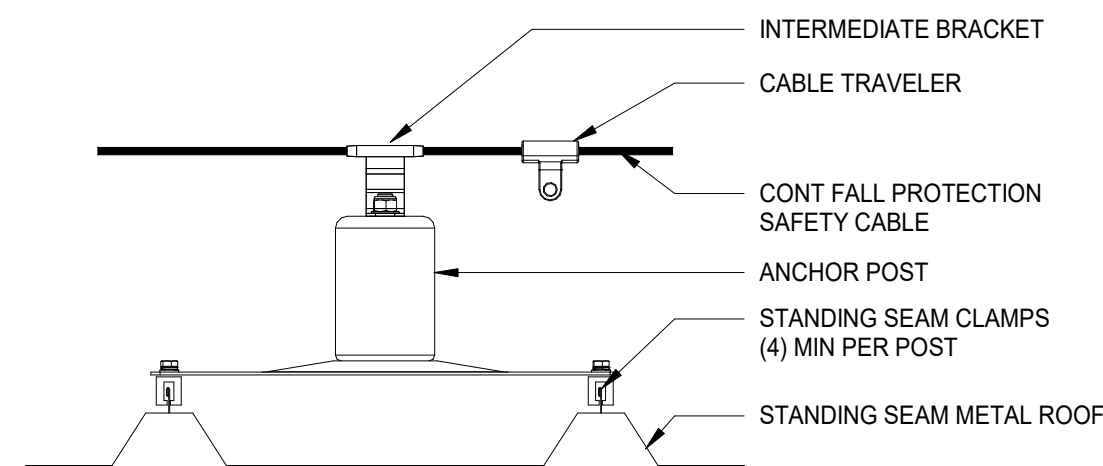
File Path:

Plot Date: 1/22/2026 2:45:39 PM

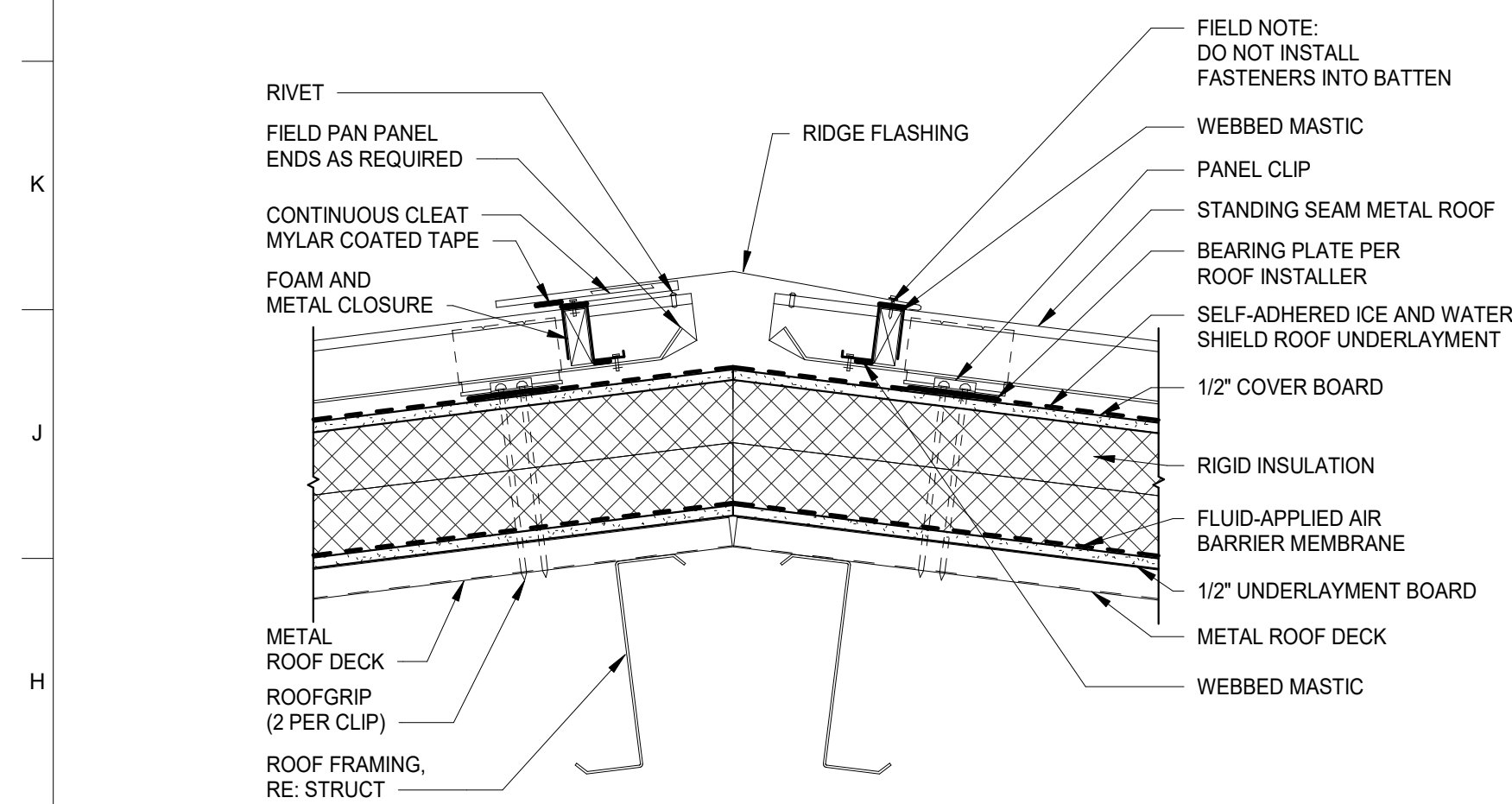
C:\Users\m5ecellm\OneDrive - US Army Corps of Engineers\Documents\EANG_512203_A_3BAYH_RVT22_m5ecellm.rvt



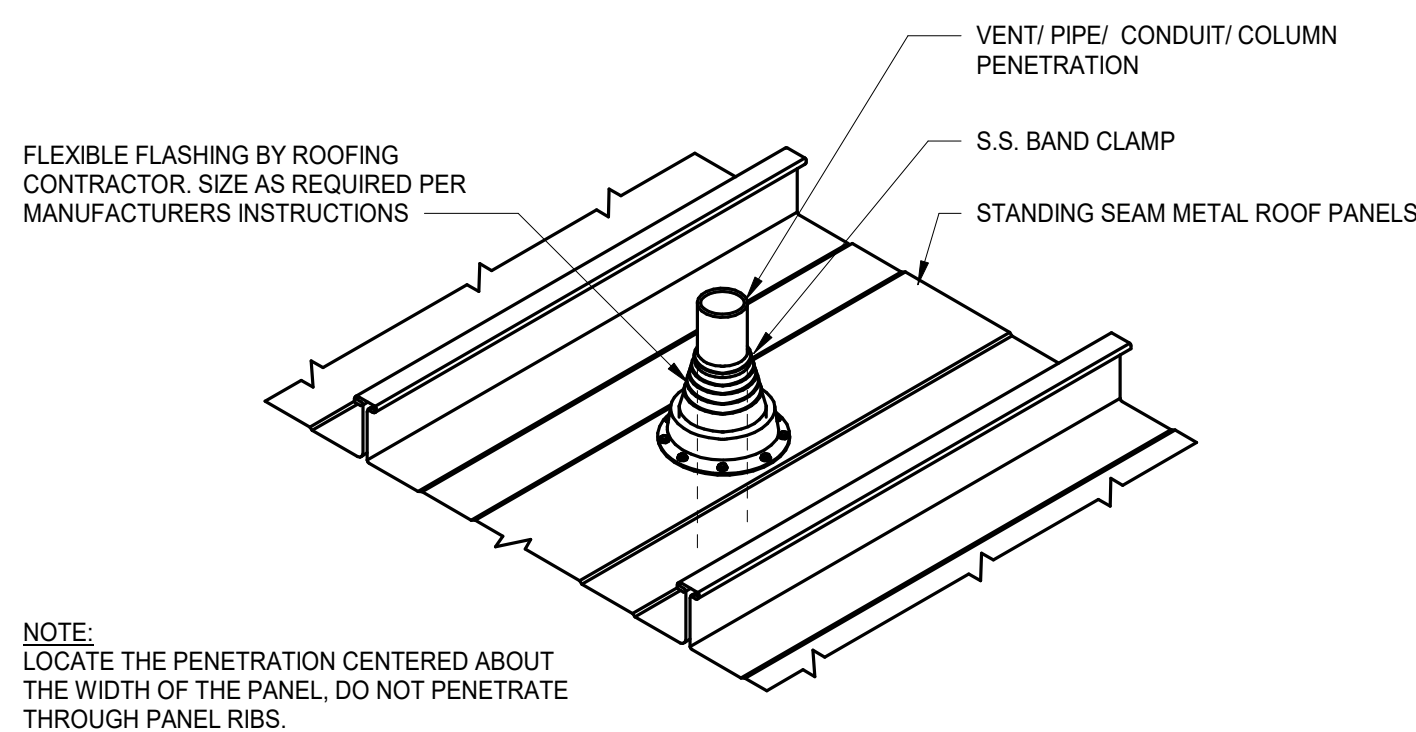
(M1) FALL PROTECTION - END



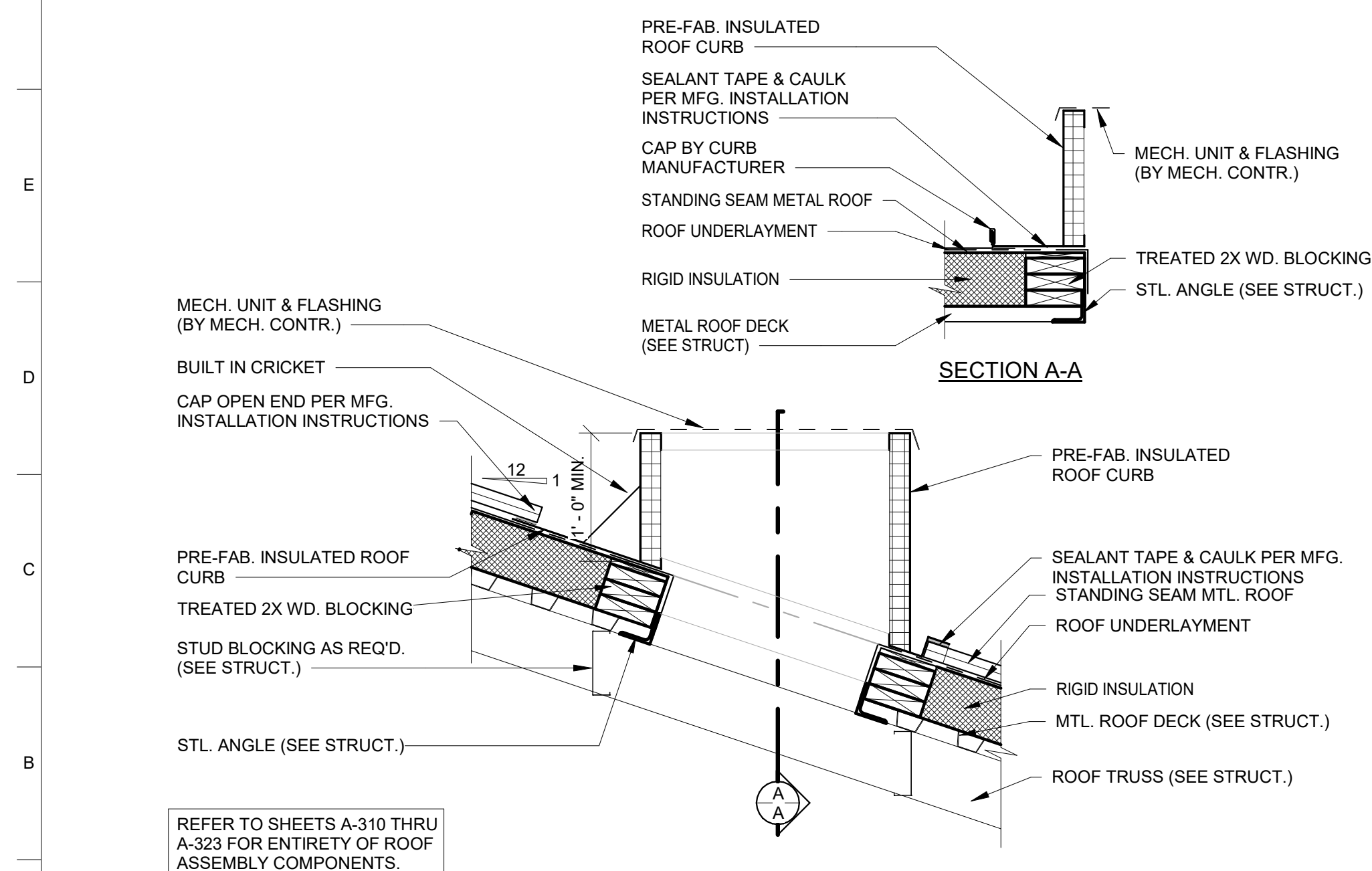
M8 FALL PROTECTION - INTERMEDIATE



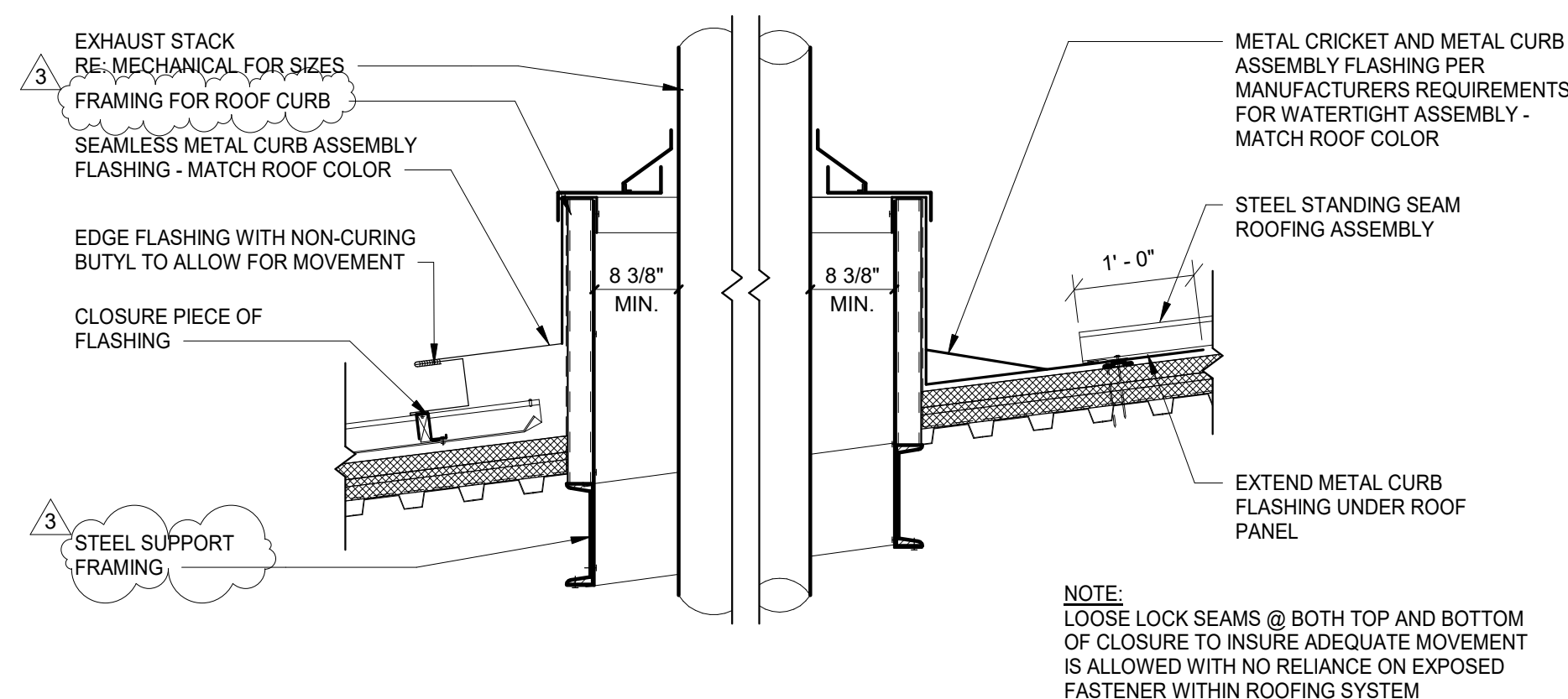
G1 STANDING SEAM METAL ROOF RIDGE



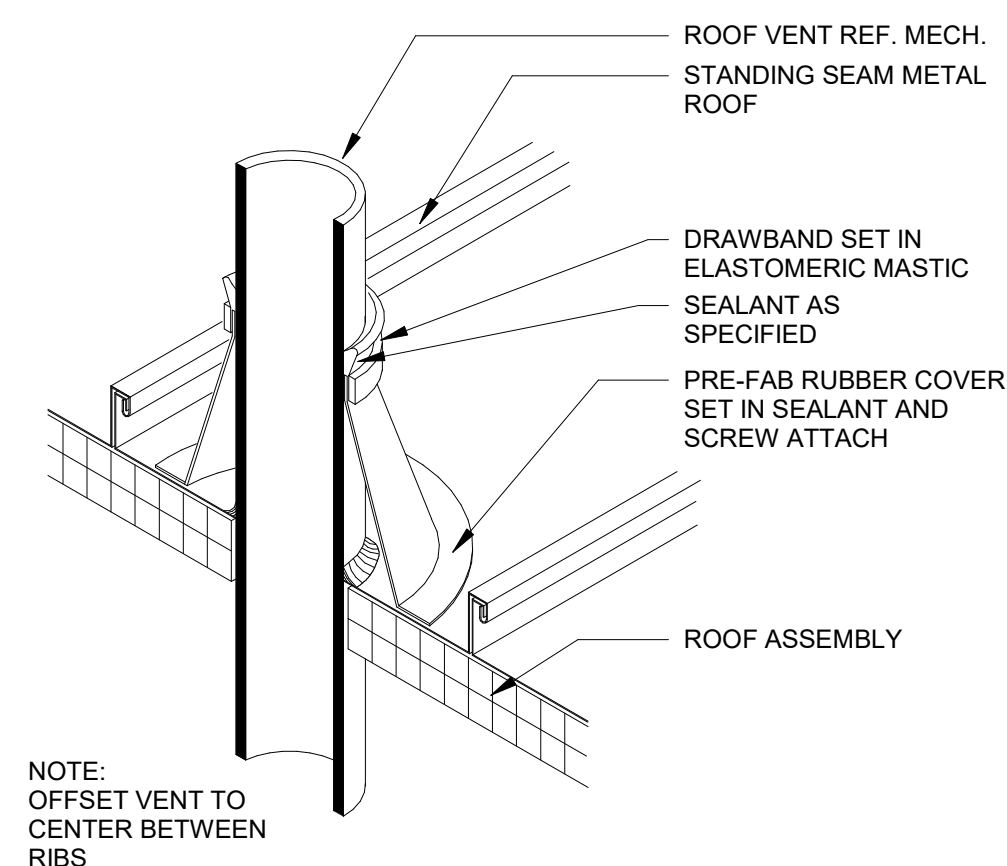
G8 STANDING SEAM ROOF PENETRATION



A1 STANDING SEAM METAL ROOF CURB



A8 EXHAUST STACK SECTION



VTR DETAIL



US Army Corps
of Engineers ®

[illegible]

DESIGNED BY: C. C. LONGACRE	ISSUE DATE: 5 DECEMBER 2025
DRAWN BY: R. R. READER	SOLICITATION NO.: W912B126RA004
CHECKED BY: M. M. HOOVER, R.A.	CONTRACT NO.:
SUBMITTED BY: A. A. BLANKENSHIP, P.E.	PROJECT NO.: 512203
SIZE: FILE NAME: ANSI/D	512203 A 3BAYH RV722.rvt

ARMY CORPS OF ENGINEERS
TULSA DISTRICT

ENGINEERING &
CONSTRUCTION DIVISION
ENGINEERING BRANCH

ANGB - ARKANSAS
3 BAY HANGAR
PN: 512203

PENETRATION AND ROOF DETAILS

SHEET ID

A-511

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
P																				
N																				
M																				
L																				
K																				
J																				
H																				
G																				
F																				
E																				
D																				
C																				
B																				
A																				

FINISH SCHEDULE

ROOM NO	ROOM NAME	FLOOR	BASE	WALL FINISH				CEILING	REMARKS
				NORTH	EAST	SOUTH	WEST		
100	ENTRY VEST	WOM	RB-1	PT-1	PT-1	PT-1	PT-1	ACT-1	
101	CORRIDOR	RES-2	RESB-2	PT-2	PT-2	PT-2	PT-2	ACT-1	3
102	FIRE PUMP	SC	RB-1	PT-2	PT-2	PT-2	PT-2	OTS	1, 5
103	TOOL RM/ALIS STATION	RES-3	RESB-3	PT-2	PT-2	PT-2	PT-2	ACT-1	
104	ELECTRICAL	SC	RB-1	PT-2	PT-2	PT-2	PT-2	OTS	1, 5
105	MECHANICAL	SC	RB-1	PT-2	PT-2	PT-2	PT-2	OTS	1, 5
106	HOIST BAY	RES-3	RESB-3	PT-2	PT-2	PT-2	PT-2	OTS	1, 4, 6
107	VEST	RES-3	RESB-3	PT-2	PT-2	PT21	PT-2	ACT-1	
108	JAN	SC	RB-1	PT-2	PT-2	PT-2	PT-2	OTS	
109	RVE STORAGE	RES-3	RESB-3	PT-2	PT-2	PT-2	PT-2	OTS	1, 4
110	MOTHER'S RM	RES-1	RB-1	PT-1	PT-1	PT-1	PT-7	PT-4	
111	OFFICE	RES-1	RB-1	PT-1	PT-7	PT-1	PT-1	ACT-1	
112	VEST	RES-3	RESB-3	PT-2	PT-2	PT-2	PT-2	ACT-1	-
113	MAINTENANCE BAY	RES-3	RESB-3	PT-2	PT-2	PT-2	PT-2	OTS	1, 4, 6
114	ALCOVE	RES-2	RESB-2	-	PT-2	PT-2	PT-2	ACT-1	



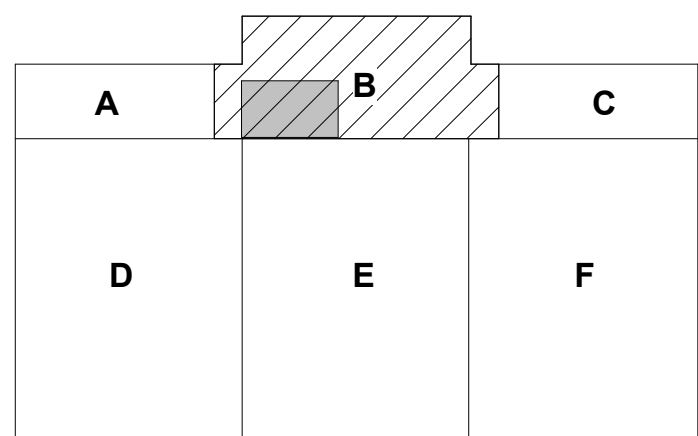
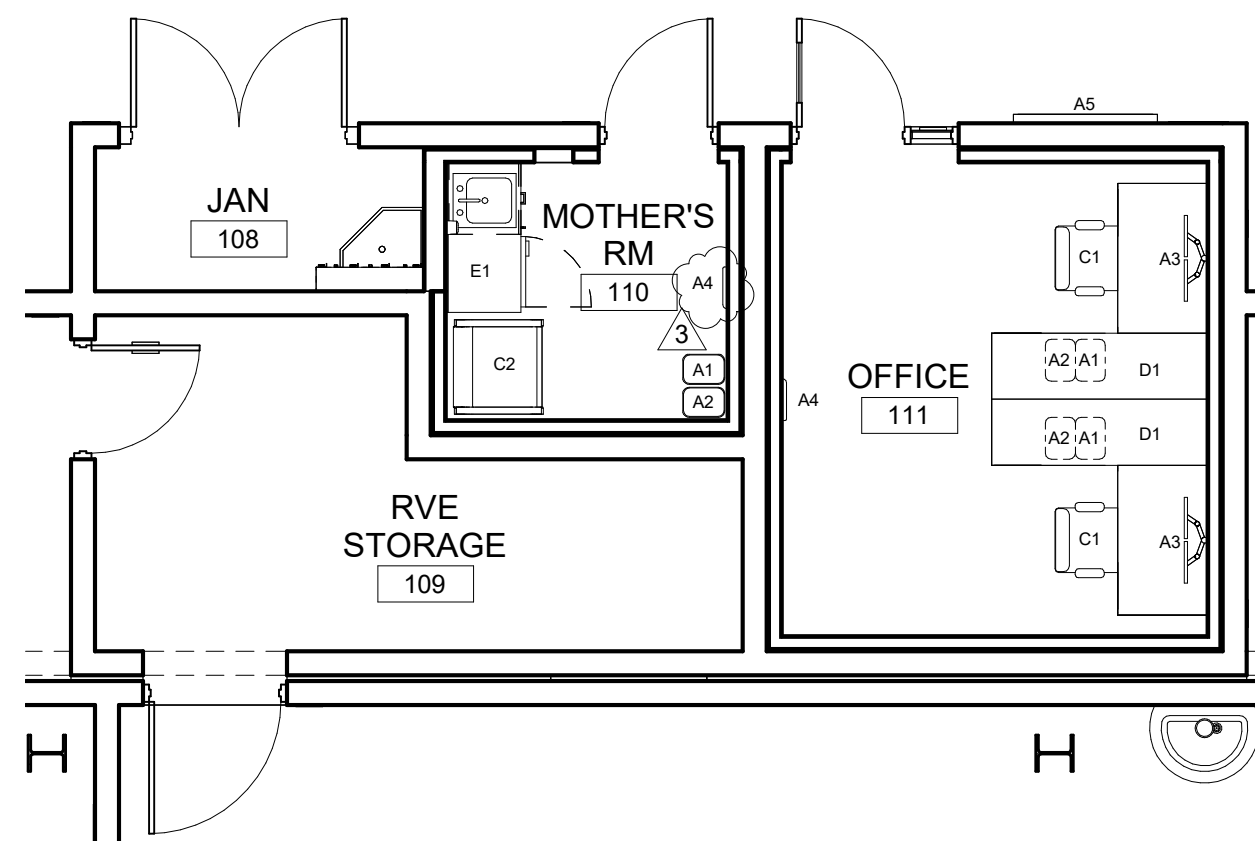
MARK	DESCRIPTION	DATE
3	AM 0003 - REVISED IN ACCORDANCE WITH AMENDMENT-3	23 JAN 2026
1	AM 0001 - REVISED ROOM/FINISH SCHEDULE; ROOM 103 REMOVED INSIDE WARD, ADDED HEIGHT TO WALL BASE RESB2 AND RESB-3.	17 DEC 2025

US ARMY CORPS OF ENGINEERS		DESIGNED BY:	ISSUE DATE:
TULSA DISTRICT		T. MANN	5 DECEMBER 2025
2408 EAST 81ST ST		R. READER	W015B76000
TULSA, OK 74137		CONTRACT NO.:	W015B76000
		M. HOOPER, R.A.	PROJECT NO.:
		SUBMITTED BY P. E.	517265
		SIZE:	FILE NAME:
		ANSI D	EANG_517203_A_38A4V_RVT22.mt

EBBING ANG-B, ARKANSAS
F-35 3 BAY HANGAR
PN: 512203

SHEET ID

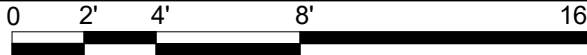
A-711



PLAN NORTH

KEY PLAN

ENLARGED FURNITURE PLAN

$$3/16'' = 1'-0''$$


GENERAL FURNITURE AND EQUIPMENT NOTES

3. FOR ARCHITECTURAL GENERAL NOTES, MATERIAL LEGEND, AND ABBREVIATIONS, REFER TO SHEET G-004.
2. REFER TO ARCHITECTURAL FLOOR PLANS FOR BUILDING LAYOUT, DIMENSIONS AND COORDINATION TO BUILDING SYSTEMS AND STRUCTURE.
3. REFER TO ELECTRICAL DRAWINGS FOR COORDINATION OF THE LIGHTING, POWER, DATA, COMMUNICATIONS AND LOCATIONS OF OTHER WALL AND FLOOR MOUNTED ELECTRICAL DEVICES AND EQUIPMENT FOR COORDINATION TO FURNITURE LAYOUTS. CONTRACTOR MUST IDENTIFY ANY CONFLICTS WITH FURNITURE LAYOUTS.
4. REFER TO MECHANICAL DRAWINGS FOR COORDINATION OF PLUMBING AND HVAC SYSTEMS TO FURNITURE LAYOUTS, THERMOSTATS, DIFFUSERS AND ACCESS PANELS MUST NOT CONFLICT WITH FURNITURE LAYOUTS. CONTRACTOR MUST IDENTIFY ANY CONFLICTS WITH FURNITURE LAYOUTS.
5. FURNITURE, FIXTURES AND EQUIPMENT (FF&E) DRAWINGS PROVIDED FOR COORDINATION WITH BUILDING SYSTEMS ONLY.
6. REFER TO FF&E PACKAGE FOR FURNITURE PROCUREMENT INFORMATION AND SPECIFICATION.
7. FIELD VERIFY ALL BUILDING CONDITIONS PRIOR TO INSTALLATION OF FF&E.
8. FF&E CONTRACTOR TO FIELD VERIFY ALL MEASUREMENTS AND SITE CONDITIONS TO ENSURE PROPER FIT OF ALL FF&E. FURNISHINGS MUST NOT OVERLAP OR OBSTRUCT DOOR FRAMES, WALL SWITCHES, THERMOSTATS OR OTHER WALL MOUNTED ITEMS. MODIFICATIONS TO FURNISHINGS LAYOUTS REQUIRED TO MEET BUILDING CONDITIONS AT TIME OF INSTALLATION MUST BE THE RESPONSIBILITY OF THE FF&E CONTRACTOR. ALL MODIFICATIONS MUST BE APPROVED IN WRITING BY A GOVERNMENT APPROVED REPRESENTATIVE PRIOR TO INSTALLATION OF THE FURNISHINGS.
9. FURNITURE INSTALLER/CONTRACTOR MUST COORDINATE POWER/COM/DATA CONNECTIONS WITH ELECTRICAL CONTRACTOR PRIOR TO INSTALLATION OF ELECTRIFIED FURNISHINGS.
10. INSTALL BULLETIN BOARDS AT 54" TO THE MID-HEIGHT OF THE BOARD.
11. INSTALL CLOCKS AT 8'-0" A.F.F. TO CENTER OF CLOCK UNLESS OTHERWISE NOTED.
12. PERSONAL WASTE (A1) TO BE AT EACH DESK IN OFFICE.
13. PERSONAL RECYCLING RECEPTACLE (A2) TO BE AT EACH DESK IN OFFICE.
14. ALL FF&E REFLECTED IN THE DRAWINGS AND FF&E PACKAGE IS PROVIDED AS BASIS OF DESIGN.

FF&E SCHEDULE

ITEM CODE	ITEM DESCRIPTION
ACCESSORIES	
A1	WASTE RECEPTACLE, PERSONAL - *IN OFFICE, LOCATED UNDER DESK
A2	RECYCLING RECEPTACLE, PERSONAL - *IN OFFICE, LOCATED UNDER DESK
A3	MONITOR ARM
A4	WALL CLOCK
A5	BULLETIN BOARD
CHAIRS & SEATING	
C1	TASK CHAIR, HARD CASTERS
C2	RECLINER
DESKS	
D1	DESK, 6'X6' L-SHAPE - WITH LOCKABLE FILE CABINET/STORAGE
EQUIPMENT	
E1	REFRIGERATOR - UNDERCOUNTER



**US Army Corps
of Engineers ®**

[illegible]

ISSUE DATE:	5 DECEMBER 2025
SOLICITATION NO.:	W912B/26RA004
CONTRACT NO.:	
PROJECT NO:	512203
DESIGNED BY:	T. MANN
DRAWN BY:	R. READER
CHECKED BY:	M. M. HOOPER, R.A.
SUBMITTED BY:	A. BLANKENSHIP, P.E.
SIZE:	EANG 512203 A 38AYH RV122.rvt
FILE NAME:	ANSID

US ARMY CORPS OF ENGINEERS
TULSA DISTRICT
2400 EAST 94TH ST

ENGINEERING &
CONSTRUCTION DIVISION
ENGINEERING BRANCH

EBBING ANGB - ARKANSAS
F-35: 3 BAY HANGAR
PN: 512203

ENLARGED FURNITURE PLAN - AREA B

SHEET ID

I-102

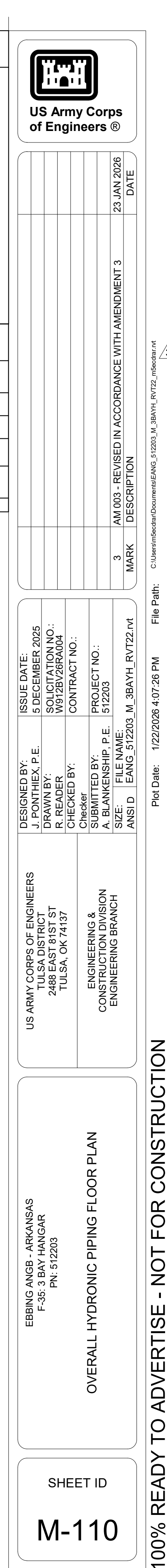
100% READY TO ADVERTISE - NOT FOR CONSTRUCTION

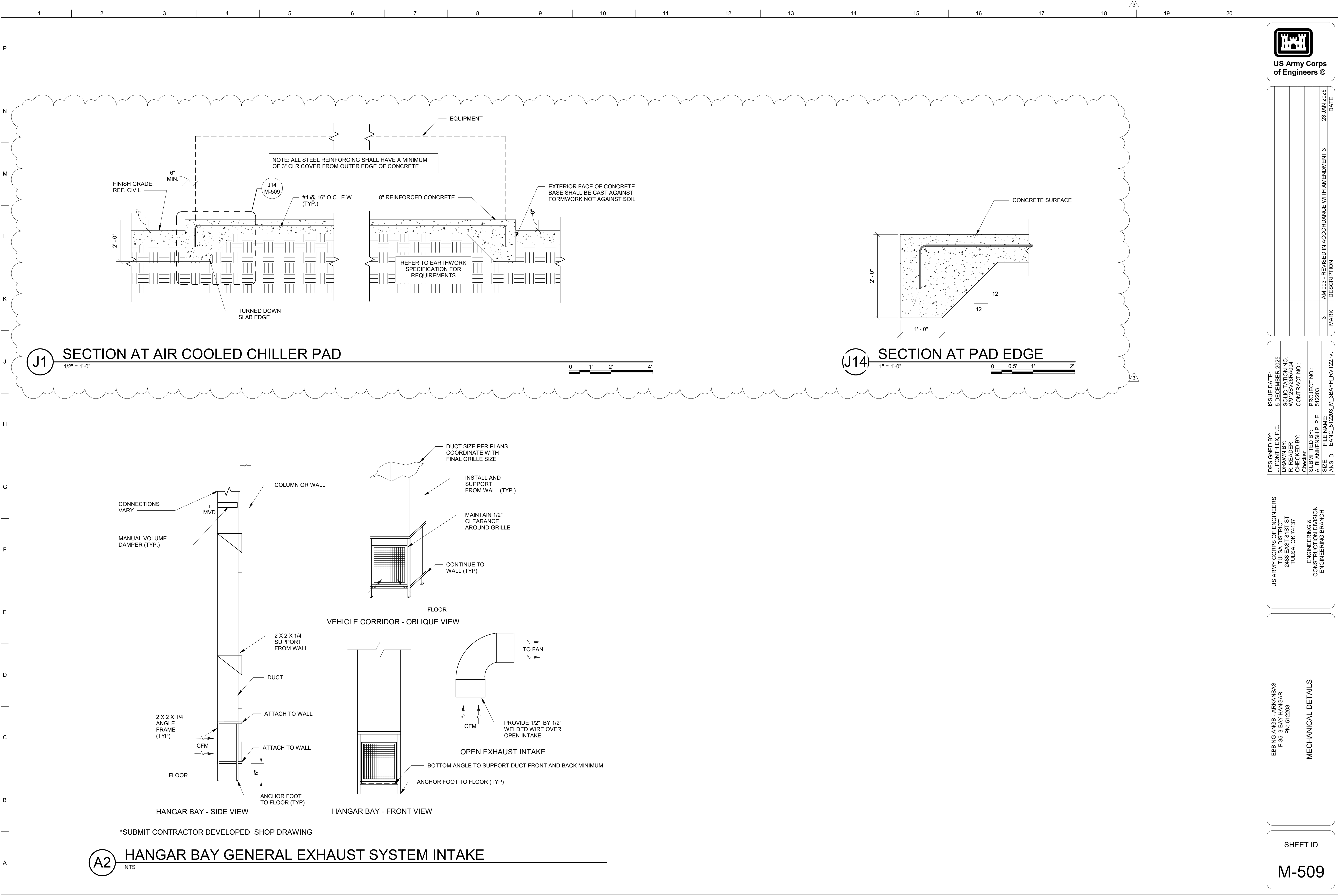
C:\Users\mSecettm\OneDrive - US Army Corps of Engineers\Documents\EANG_512203_A_3BAYH_RVT22_mSecettm.rvt

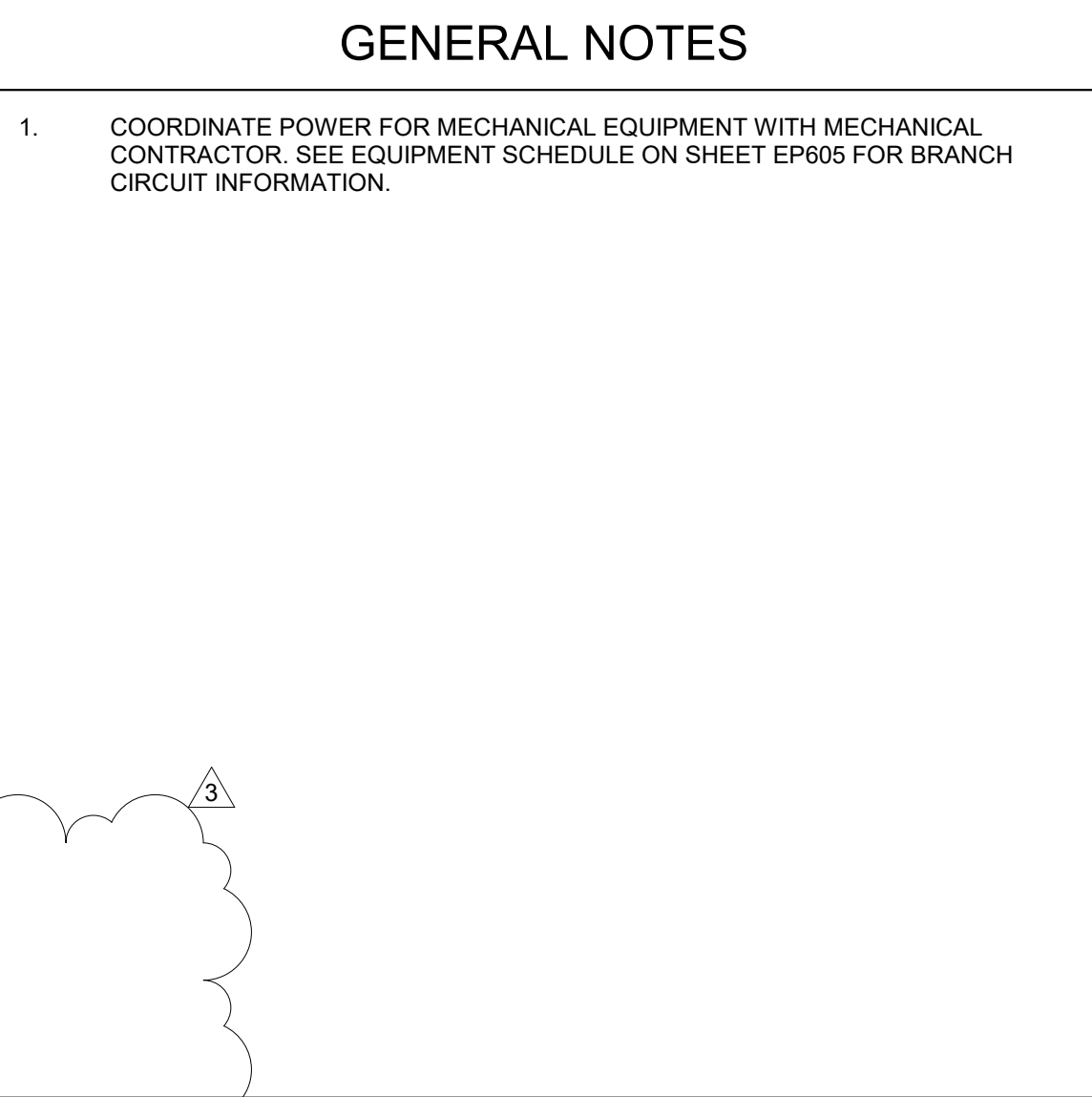
File Path:

Plot Date: 1/23/2026 12:05:40 AM

OR







3	AM 0003 - REVISED IN ACCORDANCE WITH AMENDMENT 3		23 JAN 2026
MARK	DESCRIPTION		DATE

US ARMY CORPS OF ENGINEERS TULSA DISTRICT 2448 EAST 81ST ST TULSA, OK 74137	DESIGNED BY:	C. VELOZ	ISSUE DATE:	5 DECEMBER 2025
	DESIGNED BY:	C. VELOZ	WARRANT NO.:	
	CHECKED BY:	S. KUNAPATI, P.E.	CONTRACT NO.:	
	SUBMITTED BY:		PROJECT NO.:	152205
ENGINEERING & CONSTRUCTION DIVISION ENGINEERING BRANCH	SIZE:	FILE NAME:	EANG_512205_E_38AYH_RV12Z.mt	

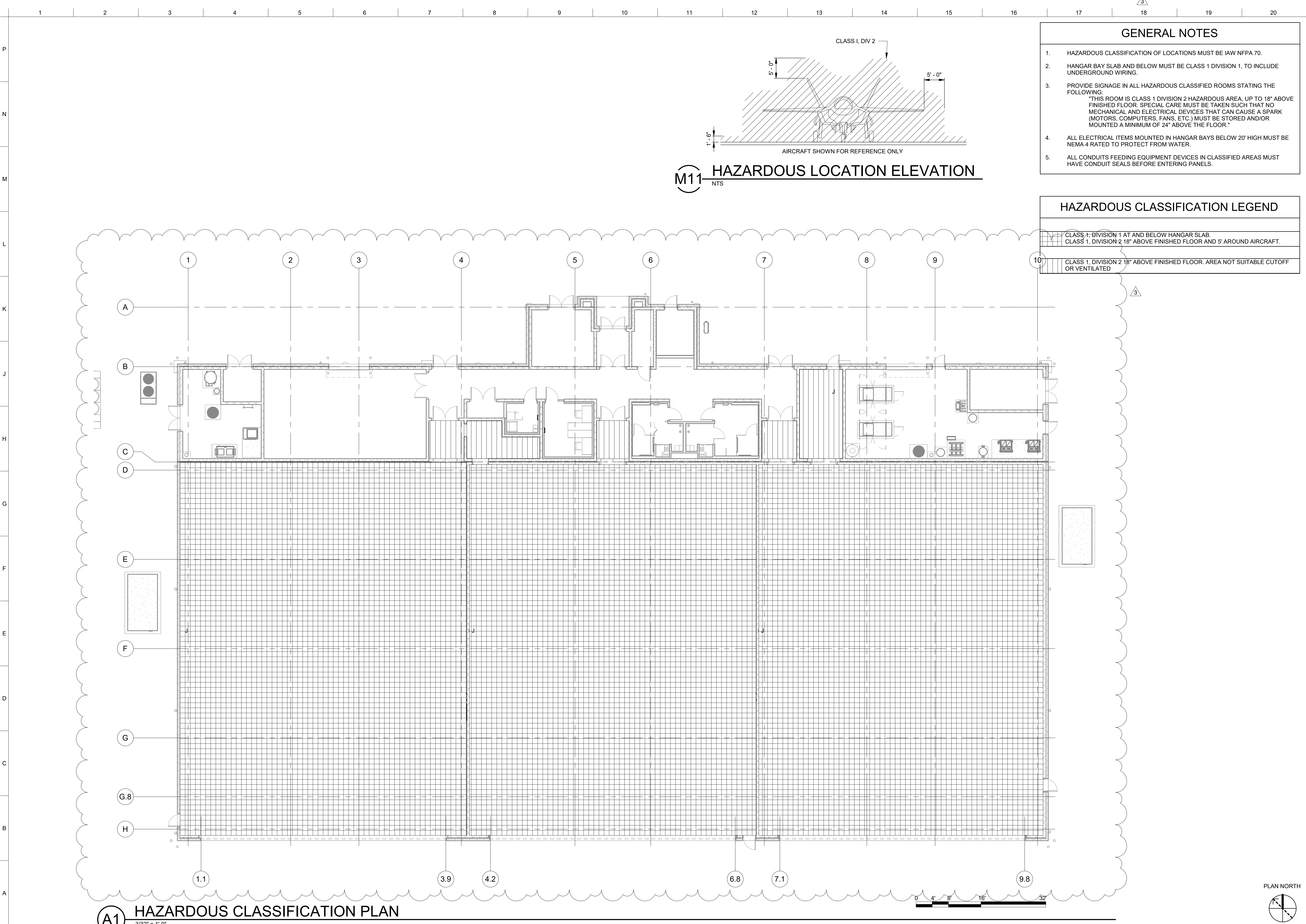
EBBING ANGB - ARKANSAS
F-35: 3 BAY HANGAR
PN: 512203

SHEET ID

EP110

100% READY TO ADVERTISE - NOT FOR CONSTRUCTION

Plot Date:	1/23/2026 9:40:46 AM	File Path:	C:\Users\m5eodes\Documents\EANG_512103_E_3BAYH_RVT22_m5eodesv.nt
------------	----------------------	------------	--



- GENERAL NOTES**
- HAZARDOUS CLASSIFICATION OF LOCATIONS MUST BE IAW NFPA 70.
 - HANGAR BAY SLAB AND BELOW MUST BE CLASS 1 DIVISION 1, TO INCLUDE UNDERGROUND WIRING.
 - PROVIDE SIGNAGE IN ALL HAZARDOUS CLASSIFIED ROOMS STATING THE FOLLOWING:
"THIS ROOM IS CLASS 1 DIVISION 2 HAZARDOUS AREA, UP TO 18" ABOVE FINISHED FLOOR. SPECIAL CARE MUST BE TAKEN SUCH THAT NO MECHANICAL AND ELECTRICAL DEVICES THAT CAN CAUSE A SPARK (MOTORS, COMPUTERS, FANS, ETC.) MUST BE STORED AND/OR MOUNTED A MINIMUM OF 24" ABOVE THE FLOOR."
 - ALL ELECTRICAL ITEMS MOUNTED IN HANGAR BAYS BELOW 20' HIGH MUST BE NEMA 4 RATED TO PROTECT FROM WATER.
 - ALL CONDUITS FEEDING EQUIPMENT DEVICES IN CLASSIFIED AREAS MUST HAVE CONDUIT SEALS BEFORE ENTERING PANELS.

HAZARDOUS CLASSIFICATION LEGEND

	CLASS 1, DIVISION 1 AT AND BELOW HANGAR SLAB. CLASS 1, DIVISION 2 18" ABOVE FINISHED FLOOR AND 5' AROUND AIRCRAFT.
	CLASS 1, DIVISION 2 18" ABOVE FINISHED FLOOR. AREA NOT SUITABLE CUTOFF OR VENTILATED

US Army Corps of Engineers

ISSUE DATE: 5 DECEMBER 2025	DESIGNED BY: C. VELOZ	US ARMY CORPS OF ENGINEERS TULSA DISTRICT 2488 EAST 81ST ST TULSA, OK 74137
SOLICITATION NO.: 512203	DRAWN BY: S. KUNAPILLI	HAZARDOUS CLASSIFICATION PLAN
CONTRACT NO.:	CHECKED BY: S. KUNAPILLI, P.E.	
PROJECT NO.: 512203	SUBMITTED BY:	
FILE NAME: EANG_512203_E_3BAYH_RVT22.rvt	SIZE: ANSI D	ENGINEERING & CONSTRUCTION DIVISION ENGINEERING BRANCH

3	AM 0003 - REVISED IN ACCORDANCE WITH AMENDMENT 3	23 JAN 2026
MARK	DESCRIPTION	DATE

100% READY TO ADVERTISE - NOT FOR CONSTRUCTION

SHEET ID
EP117