DEPARTMENT OF THE NAVY
NAVAL FACILITIES ENGINEERING COMMAND
1322 PATTERSON AVENUE, SE SUITE 1000
WASHINGTON NAVY YARD DC 20374-5065

IN REPLY REFER TO

26 January 2017

From: Commander, Naval Facilities Engineering Command

Subj: INTERIM TECHNICAL GUIDANCE (ITG 2017-01) - APPLICATION OF CYBERSECURITY TO FACILITY-RELATED CONTROL SYSTEMS

Ref: (a) DoDI 8500.01, Cybersecurity, March 2014
(b) DoDI 8510.01, Risk Management Framework (RMF) for DoD Information Technology, March 2014
(c) CNIC/NAVFAC JOINT LETTER "Cybersecurity Tasking For Ashore Control Systems", 06 October 2016
(d) UFC 4-010-06 Cybersecurity of Facility-Related Control Systems, 19 September 2016

Encl: (1) UFGS 25 50 00.00 20 CYBERSECURITY OF FACILITY-RELATED CONTROL SYSTEMS
(2) Cybersecurity Hygiene Checklist (Contractor Version)

1. Purpose. This ITG provides the basic criteria guidance concerning the implementation of Cybersecurity to Facility-Related Control Systems for projects currently under design and construction.

2. Background. A control system (CS) typically consists of network capable digital controllers and user interfaces that are used to monitor and possibly control equipment. There are many types of control systems ranging from building control systems to manufacturing control systems to weapon control systems, all with different names and terminology. Facility-related control systems are a subset of control systems that are used to monitor and control equipment and systems, such as building control systems, utility control systems, electronic security systems, and fire and life safety systems. Per the requirements of References (a) and (b), facility control systems must be cybersecured.

a. CNIC and NAVFAC issued reference (c) to inventory, assess, interim secure, secure, and continuously monitor all facility control systems on Navy installations in their respective regions.

b. This effort will be conducted largely by the Echelon IV NAVFAC Public Works (PW) and the Command Information Office (CIO).

3. Discussion.

a. For projects currently under design and construction, ITG 2017-01, through UFGS 25 50 00.00 20,incorporates elements of the NAVFAC Cybersecurity Hygiene Checklist into contract specifications for control systems. These elements will facilitate achieving an Interim Secure cybersecurity level and lessens the effort for PW/CIO when these facilities are accepted into the CNIC inventory. The elements of the Cybersecurity Hygiene Checklist do not require extensive design or construction effort.

b. Reference (d), UFC 4-010-06, CYBERSECURITY OF FACILITY-RELATED CONTROL SYSTEMS was issued 19 September 2016 and is available on the Whole Building Design Guide website (www.wbdg.org). The Tri-Service Unified Facility Guide Specification (UFGS) containing detailed cybersecurity requirements is not scheduled for release until early FY18 (November 2017).

4. Technical Guidance. ITG 2017-01, including UFGS 25 50 00.00 20, will remain in effect until the Tri-Service cybersecurity UFGS is posted on the Whole Building Design Guide in early FY18.

5. Action.

a. This ITG applies to all design and construction, renovation, and repair of new and existing facilities currently under design and construction that result in DoN real property assets, regardless of funding source. Enclosure (1) contains UFGS 25 50 00.00 20, which requires the construction contractor to complete the Cybersecurity Hygiene Checklist. Coordinate requirements with other project specifications having facility-related control systems as required by enclosure (1).

b. Incorporate the requirements of UFGS 25 50 00.00 20 for all FY17 and earlier Navy MILCON (e.g., MCON, ECIP, and UMC) projects where project execution is

i. In Design:

1. Beyond 35% design and without Design Release

2. Between Design Release and Contract Award (evaluate the impacts of a pre-award amendment versus a post-award modification)

ii. In Construction:

1. Prior to DBB Pre-Construction Meeting/DB Final Design Acceptance (post award modification)

2. Between DBB Pre-Construction Meeting/DB Post-Award Kick-off Meeting and RedZone meeting only if there are not significant project impacts to schedule and cost (post-award modification)

c. Incorporate the requirements of UFGS 25 50 00.00 20 for all non-MILCON Navy (e.g., O&M,N) projects where project execution is:

i. Beyond 35% design and without Design Release

ii. Between Design Release and DBB Pre-Construction Meeting/DB Post Award Kickoff Meeting (evaluate the impacts of a pre-award amendment versus a post-award modification)

iii. Between DBB Pre-Construction Meeting/DB Post-Award Kick-off Meeting and RedZone meeting only if there are not significant project impacts to schedule and cost (post-award modification)

6. Coordination. This ITG has been coordinated with NAVFAC Mechanical, Electrical, and Fire Protection Engineering (CI4) communities of practice. ITGs are published by the NAVFAC Engineering Criteria and Programs Office (CI1) as part of the NAVFAC Criteria Program and are available in PDF and SpecsIntact format on the WBDG at https://www.wbdg.org/ffc/navy-navfac/interim-technical-guidance-itg.

7. Points of Contact. For clarification or additional information related to this subject, please contact either Emil Consolacion, P.E., DSN 262-4205, Comm. (757) 322-4205, e-mail emil.consolacion@navy.mil, Dave Phelps, P.E. DSN 262-4327, Comm. (757) 322-4327, e-mail william.phelps@navy.mil, or Joseph Simone, P.E., DSN 325-9177, Comm. (202) 685-9177, e-mail joseph.simone@navy.mil.

BERNIE J. DENEKE, P.E.
By direction

Distribution:
NAVFAC (CHE, CIBL, CIO, AMBL, PWBL)
NAVFAC Atlantic (CIBL, CIO, AMBL, PWBL)
NAVFAC Pacific (CIBL, CIO, AMBL, PWBL)
NAVFAC Midlant (CIBL, CIO, AMBL, PWBL)

NAVFAC Southeast (CIBL, CIO, AMBL, PWBL)
NAVFAC Washington (CIBL, CIO, AMBL, PWBL)
NAVFAC EURAFSWA (CIBL, CIO, AMBL, PWBL)
NAVFAC Northwest (CIBL, CIO, AMBL, PWBL)
NAVFAC Southwest (CIBL, CIO, AMBL, PWBL)
NAVFAC Far East (CIBL, CIO, AMBL, PWBL)
NAVFAC Hawaii (CIBL, CIO, AMBL, PWBL)
NAVFAC Marianas (CIBL, CIO, AMBL, PWBL)
NAVFAC EXWC (CIBL, CIO, PWBL)

Copy to:
CMC Washington
HQ USMC (MCICOM)

****
USACE / NAVFAC / AFCEC / NASA UFGS-25 50 00.00 20 (01/2017)

Preparing Activity: NAVFAC NEW

UNIFIED FACILITIES GUIDE SPECIFICATIONS

References are in agreement with UMRL dated 11/2016
****

SECTION 25 50 00.00 20

CYBERSECURITY OF FACILITY-RELATED CONTROL SYSTEMS
01/17

****
NOTE: This guide specification covers the requirements for a Construction Contractor version of the NAVFAC Cybersecurity Hygiene Checklist, required by the Joint CNIC/NAVFAC CYBERSECURITY TASKING FOR ASHORE CONTROL SYSTEMS (dated 06 October 2016), for facilities that are in various phases of design or construction (i.e., not yet in CNIC's existing inventory). These requirements are based on basic cybersecurity hygiene practices and have minimal impact to construction cost and schedule; however, they have a major benefit to delivering interim secure facilities.

Adhere to UFC 1-300-02 Unified Facilities Guide Specifications (UFGS) Format Standard when editing this guide specification or preparing new project specification sections. Edit this guide specification for project specific requirements by adding, deleting, or revising text. For bracketed items, choose applicable items(s) or insert appropriate information.

Remove information and requirements not required in respective project, whether or not brackets are present.

Comments, suggestions and recommended changes for this guide specification are welcome and should be as a Criteria Change Request (CCR).
****

****
NOTE: Use this specification on project specifications where cybersecurity verification is required for facility-related control systems.

The following sections contain control systems that must be secure:

Section 14 21 13 ELECTRIC TRACTION FREIGHT ELEVATORS
Section 14 21 23 ELECTRIC TRACTION PASSENGER

ELEVATORS
Section 14 24 13 HYDRAULIC FREIGHT ELEVATORS
Section 14 24 23 HYDRAULIC PASSENGER ELEVATORS
Section 21 13 19.00 20 [DELUGE] [PREACTION] FIRE SPRINKLER SYSTEMS
Section 21 13 20.00 20 FOAM FIRE EXTINGUISHING FOR AIRCRAFT HANGARS
Section 21 13 21.00 20 FOAM FIRE EXTINGUISHING FOR FUEL TANK PROTECTION
Section 21 13 22.00 20 FOAM FIRE EXTINGUISHING FOR HAZ/FLAM MATERIAL FACILITY
Section 21 13 24.00 10 AQUEOUS FILM-FORMING FOAM (AFFF) FIRE PROTECTION SYSTEM
Section 21 21 01.00 20 CARBON DIOXIDE FIRE EXTINGUISHING (HIGH PRESSURE)
Section 21 21 02.00 20 CARBON DIOXIDE FIRE EXTINGUISHING (LOW PRESSURE)
Section 21 22 00.00 20 HALON 1301 FIRE EXTINGUISHING
Section 21 22 00.00 40 CLEAN AGENT FIRE EXTINGUISHING SYSTEMS
Section 21 30 00 FIRE PUMPS
Section 23 09 23.13 20 BACnet DIRECT DIGITAL CONTROL SYSTEMS FOR HVAC
Section 26 05 33 DOCKSIDE POWER CONNECTION STATIONS
Section 26 11 13.00 20 PRIMARY UNIT SUBSTATIONS
Section 26 11 16 SECONDARY UNIT SUBSTATIONS
Section 26 13 00 SF6/HIGH-FIREPOINT FLUIDS INSULATED PAD-MOUNTED SWITCHGEAR
Section 26 13 01 PAD-MOUNTED DEAD-FRONT AIR INSULATED SWITCHGEAR
Section 26 20 00 INTERIOR DISTRIBUTION SYSTEM
Section 26 23 00 LOW VOLTAGE SWITCHGEAR
Section 26 24 13 SWITCHBOARDS
Section 26 27 14.00 20 ELECTRICITY METERING
Section 26 29 23 VARIABLE FREQUENCY DRIVE SYSTEMS UNDER 600 VOLTS
Section 26 31 00 SOLAR PHOTOVOLTAIC (PV) COMPONENTS
Section 26 32 13.00 20 SINGLE OPERATION GENERATOR SETS
Section 26 33 53.00 20 UNINTERRUPTIBLE POWER SUPPLY (UPS)
Section 26 35 43 400-HERTZ (HZ) SOLID STATE FREQUENCY CONVERTER
Section 26 36 23.00 20 AUTOMATIC TRANSFER SWITCHES
Section 26 51 00 INTERIOR LIGHTING
Section 26 56 00 EXTERIOR LIGHTING
Section 27 21 00.00 20 INTERCOMMUNICATION SYSTEM
Section 27 52 23.00 20 NURSE CALL SYSTEM
Section 27 52 24 NURSE CALL SYSTEMS (DRAFT)
Section 28 10 05 ELECTRONIC SECURITY SYSTEMS
Section 28 20 02 CENTRAL MONITORING SERVICES FOR ELECTRONIC SECURITY SYSTEMS
Section 28 31 02.00 20 FIRE ALARM REPORTING SYSTEMS-DIGITAL COMMUNICATIONS
Section 28 31 33.13 20 EXTERIOR FIRE REPORTING SYSTEM, RADIO TYPE
Section 28 31 63.00 20 ANALOG/ADDRESSABLE INTERIOR FIRE ALARM SYSTEM

Section 28 31 74.00 20 INTERIOR FIRE DETECTION AND ALARM SYSTEM
Section 28 31 76 INTERIOR FIRE ALARM AND MASS NOTIFICATION SYSTEM
Section 33 11 00 WATER UTILITY DISTRIBUTION PIPING
Section 33 71 01 OVERHEAD TRANSMISSION AND DISTRIBUTION
Section 40 95 00 PROCESS CONTROL

****

PART 1 GENERAL

1.1 SUBMITTALS

****
When this specification is used, add the following to Section 01 30 00 paragraph PRECONSTRUCTION MEETING:

"1.9.1 Cybersecurity of Control Systems

Discuss Cybersecurity of building control system requirements and submittals as required for Section 25 50 00.00 20 CYBERSECURITY OF FACILITY-RELATED CONTROL SYSTEMS."
****

Government approval is required for submittals with a "G" designation; submittals not having a "G" designation are [for Contractor QC approval.][for information only. When used, a designation following the "G" designation identifies the office that will review the submittal for the Government.] Submittals with an "S" are for inclusion in the Sustainability Notebook, in conformance to Section 01 33 29, SUSTAINABITY REQUIREMENTS. Submit the following in accordance with Section 01 33 00 SUBMITTAL PROCEDURES:

SD-05 Design Data

Cybersecurity Plan

SD-09 Manufacturer's Field Reports

Cybersecurity Hygiene Report

1.2 QUALITY ASSURANCE

1.2.1 Cybersecurity Plan

****
NOTE: Provide office code, usually CI04, contact phone number, and address of NAVFAC CIO in brackets.
****

Provide a cybersecurity plan that lists equipment and systems to be verified for Cybersecurity. The plan must list the individuals who will

perform the Cybersecurity requirements. The plan must include all requirements of the Cybersecurity Hygiene Checklist and if required, other proposed cybersecurity requirements from the equipment manufacturer. Provide the plan a minimum of 60 days before the anticipated site visit for the cybersecurity field verifications. In addition to the requirements of Section 01 33 00 SUBMITTAL PROCEDURES, provide one copy of the Cybersecurity Plan, for information only, to [ ].

1.2.2 Cybersecurity Hygiene Report

****
NOTE: Provide office code, usually CI04, contact phone number, and address of NAVFAC CIO in brackets.
****

Provide a cybersecurity hygiene report that documents the compliance with the requirements identified in paragraph CYBERSECURITY HYGIENE REQUIREMENTS for each control system provided. In addition to the requirements of Section 01 33 00 SUBMITTAL PROCEDURES, provide one copy of the Cybersecurity Hygiene Report, for information only, to [ ].

1.2.2.1 Cybersecurity Hygiene Checklist

****
NOTE: The individual control system cybersecurity hygiene checklist must be completed by personnel that are knowledgeable in that system. This is typically expected to be the system installer.
****

Provide the Cybersecurity Hygiene Checklist in the report (TO DOWNLOAD THIS FORM, SEE UFGS GRAPHICS at http://www.wbdg.org/ccb/NAVGRAPH/graphtoc.pdf.) and any supporting documentation for each control system provided. Supporting documentation must include all configuration settings and diagrams for each control system. Compile the checklist from each section into a single report.

1.2.3 Facility-related Control System Requirements

****
NOTE: Add to each of the listed specifications used, with correct SI tags, the following paragraphs:

"1.X SUBMITTALS

SD-09 Manufacturer's Field Reports

Cybersecurity Hygiene Checklist"

"3.X CYBERSECURITY

Provide completed Cybersecurity Hygiene Checklist in accordance with Section 25 50 00.00 20 CYBERSECURITY OF FACILITY-RELATED CONTROL SYSTEMS."

This paragraph supersedes existing paragraphs titled "cybersecurity" that related requirements to SCADA

systems.

NOTE: Add to the following list any specification sections that may have controls and are not listed, or have had controls added for specified equipment, example: time of usage controllers for electric vehicle chargers.

****

Incorporate each of the requirements identified in paragraph CYBERSECURITY HYGIENE REQUIREMENTS into applicable equipment and systems specified in the following sections:

[a. Section 14 21 13 ELECTRIC TRACTION FREIGHT ELEVATORS

][b. Section 14 21 23 ELECTRIC TRACTION PASSENGER ELEVATORS

][c. Section 14 24 13 HYDRAULIC FREIGHT ELEVATORS

][d. Section 14 24 23 HYDRAULIC PASSENGER ELEVATORS

][e. Section 21 13 19.00 20 [DELUGE] [PREACTION] FIRE SPRINKLER SYSTEMS

][f. Section 21 13 20.00 20 FOAM FIRE EXTINGUISHING FOR AIRCRAFT HANGARS

][g. Section 21 13 21.00 20 FOAM FIRE EXTINGUISHING FOR FUEL TANK PROTECTION

][h. Section 21 13 22.00 20 FOAM FIRE EXTINGUISHING FOR HAZ/FLAM MATERIAL FACILITY

][i. Section 21 13 24.00 10 AQUEOUS FILM-FORMING FOAM (AFFF) FIRE PROTECTION SYSTEM

][j. Section 21 21 01.00 20 CARBON DIOXIDE FIRE EXTINGUISHING (HIGH PRESSURE)

][k. Section 21 21 02.00 20 CARBON DIOXIDE FIRE EXTINGUISHING (LOW PRESSURE)

][l. Section 21 22 00.00 20 HALON 1301 FIRE EXTINGUISHING

][m. Section 21 22 00.00 40 CLEAN AGENT FIRE EXTINGUISHING SYSTEMS

][n. Section 21 30 00 FIRE PUMPS

][o. Section 23 09 23.13 20 BACnet DIRECT DIGITAL CONTROL SYSTEMS FOR HVAC

][p. Section 26 05 33 DOCKSIDE POWER CONNECTION STATIONS

][q. Section 26 11 13.00 20 PRIMARY UNIT SUBSTATIONS

][r. Section 26 11 16 SECONDARY UNIT SUBSTATIONS

][s. Section 26 13 00 SF6/HIGH-FIREPOINT FLUIDS INSULATED PAD-MOUNTED SWITCHGEAR

][t. Section 26 13 01 PAD-MOUNTED DEAD-FRONT AIR INSULATED SWITCHGEAR

][u. Section 26 20 00 INTERIOR DISTRIBUTION SYSTEM

][v. Section 26 23 00 LOW VOLTAGE SWITCHGEAR

][w. Section 26 24 13 SWITCHBOARDS

][x. Section 26 27 14.00 20 ELECTRICITY METERING

][y. Section 26 29 23 VARIABLE FREQUENCY DRIVE SYSTEMS UNDER 600 VOLTS

][z. Section 26 31 00 SOLAR PHOTOVOLTAIC (PV) COMPONENTS

][aa. Section 26 32 13.00 20 SINGLE OPERATION GENERATOR SETS

][ab. Section 26 33 53.00 20 UNINTERRUPTIBLE POWER SUPPLY (UPS)

][ac. Section 26 35 43 400-HERTZ (HZ) SOLID STATE FREQUENCY CONVERTER

][ad. Section 26 36 23.00 20 AUTOMATIC TRANSFER SWITCHES

][ae. Section 26 51 00 INTERIOR LIGHTING

][af. Section 26 56 00 EXTERIOR LIGHTING

][ag. Section 27 21 00.00 20 INTERCOMMUNICATION SYSTEM

][ah. Section 27 52 23.00 20 NURSE CALL SYSTEM

][ai. Section 27 52 24 NURSE CALL SYSTEMS (DRAFT)

][aj. Section 28 10 05 ELECTRONIC SECURITY SYSTEMS

][ak. Section 28 20 02 CENTRAL MONITORING SERVICES FOR ELECTRONIC SECURITY SYSTEMS

][al. Section 28 31 02.00 20 FIRE ALARM REPORTING SYSTEMS-DIGITAL COMMUNICATIONS

][am. Section 28 31 33.13 20 EXTERIOR FIRE REPORTING SYSTEM, RADIO TYPE

][an. Section 28 31 63.00 20 ANALOG/ADDRESSABLE INTERIOR FIRE ALARM SYSTEM

][ao. Section 28 31 74.00 20 INTERIOR FIRE DETECTION AND ALARM SYSTEM

][ap. Section 28 31 76 INTERIOR FIRE ALARM AND MASS NOTIFICATION SYSTEM

][aq. Section 33 11 00 WATER UTILITY DISTRIBUTION PIPING

][ar. Section 33 71 01 OVERHEAD TRANSMISSION AND DISTRIBUTION

][as. Section 40 95 00 PROCESS CONTROL

][at. Section [_____] [_____]

1.2.4 Cybersecurity Hygiene Requirements

Items below are organized according to the Cybersecurity Hygiene Checklist. Where the requirement corresponds with a specific Cybersecurity Hygiene Checklist task number, the reference is cited at end of the paragraph in parenthesis.

1.2.4.1 Inventory

a. Provide an inventory of all IP-based control system hardware and software using CS Inventory TEMPLATE Version 10.6 (TO DOWNLOAD THIS TEMPLATE, SEE UFGS GRAPHICS (http://www.wbdg.org/ccb/NAVGRAPH/graphtoc.pdf) (Task ID# 1)

b. Provide the latest Operation System (OS) software for the control system. (Task ID# 2)

1.2.4.2 User/Password

a. Provide non-proprietary password for wireless networks. (Task ID# 4)

b. Provide system capability to change default passwords. (Task ID# 5)

c. Separate administrator and operator accounts, permissions, and passwords. (Task ID# 7)

d. Change passwords to meet DoD password standards. (Task ID# 8)

e. Create accounts and site access grants that follow the rule of least privilege, only granting access to the level necessary for completion of approved actions. (Task ID# 9)

f. Provide restrictions to privileged accounts. (Task ID# 10)

g. Validation system for individuals with privileged access indicating they have signed privileged access form and completed background check. (Task ID# 11)

h. Provide user access rights. Increase or restrict access as needed based on access requirements. (Task ID# 12)

i. Delete unused accounts. (Task ID# 13)

j. Provide shared credentials/accounts where required. (Task ID# 14)

k. Provide recovery modes that can provide access to the system by unique accounts tied to individual users. (Task ID# 15)

l. Limit access to recovery modes to individual users with a role requiring access. (Task ID# 16)

m. Provide role based permissions. (Task ID# 17)

1.2.4.3 Process

a. Create system log files that will require cyber-preventative maintenance focusing on the following core tasks: scanning, patching,

reporting, configuration management (CM), log file analysis, and HBSS/Host Intrusion Preventions System, (HIPS). (Task ID# 23)

1.2.4.4 Connectivity

a. Ensure there is no vendor remote access. (Task ID# 24 and 25)

1.2.4.5 Physical Access

a. Provide control system components in a locked panel secured to floor/wall. Provide all keys to the Government. (Task ID# 29 and 30)

1.2.4.6 Hardware and Software

a. Remove all software not required for operation and maintenance of the product. (Task ID# 32)

PART 2 PRODUCTS

Not used.

PART 3 EXECUTION

3.1 FIELD QUALITY ASSURANCE

3.1.1 Cybersecurity Field Verification

****

NOTE: The checklist must be verified in the presence of the Government and the CIO representative when possible.

The individual control system cybersecurity field inspection must be conducted by personnel that are knowledgeable in that system, typically the system installer.

****

Field verify the cybersecurity hygiene checklist information with Contractor and Government personnel. Include the following personnel: Contractor's System Installer and Quality Control Manager, the Government's Contracting Officer Representative, including the CIO representative when available. The Contractor must contact the Contracting Officer for CIO representation. The Contracting Officer reserves the right to witness all system verifications for cybersecurity.

3.1.1.1 Cybersecurity Field Verification Request

Perform the cybersecurity field verification for applicable equipment and systems specified in the sections listed in paragraph FACILITY-RELATED CONTROL SYSTEM REQUIREMENTS. The Contracting Officer must be notified at least 15 days in advance of when the cybersecurity inspection will be done. Every item on the checklist for applicable equipment and systems specified is required to be examined for successful field verification.

3.1.1.2 Verification for Each System

Field verify the completeness of the cybersecurity hygiene checklist at the field testing of each system installation. Group the control system cybersecurity verifications to minimize the Contracting Officer witnessing effort.

-- End of Section --

Cybersecurity Hygiene Checklist

Instructions: Please check the box in the completed field when you have executed the specified task. If you are unable to or do not complete a task, please provide an explanation and rationale in the comments box.

Task ID #	Tasks	Completed? Y/N	Responsible Party	Comments
Inventory				
1	An inventory of control system hardware and software was completed.			
2	The operational community shall perform inventory checks using the provided baseline, reporting results in an actionable fashion.			
3	Provide an accurate, complete, up-to-date, and timely inventory list, also known as a baseline list, of the approved hardware and software to the operational community. Store lists based on classification level.	Not in Contract (NIC)		
User / Password				
4	Wireless networks have passwords.			
5	Changed system default passwords, as appropriate.			
6	Educate the operator/technician on their responsibility for password/account protection	Not in Contract (NIC)		
7	Separated administrator and operator accounts, permissions, and passwords, as feasible.			
8	Passwords have been changed to meet DoD password standards, if feasible.			
9	When creating accounts or granting site access, follow the rule of least privilege, only granting access to the level necessary for completion of approved actions.			
10	Privileged accounts have been reviewed and restricted as necessary.			
11	Individuals with privileged access have signed privileged access form and background check has been completed.			
12	Reviewed and provided the appropriate user access rights, increasing or restricting access as needed based on access requirements.			
13	Unused accounts have been deleted.			
14	Identified whether shared credentials/accounts are utilized or not on this control system. Document result in comments.			
15	Ensure all recovery modes that can provide access to the system may only be accessed by unique accounts tied to individual users.			
16	Unless otherwise explicitly exempted, ensure the system limits access to recovery modes to individual users with a role requiring access.			
17	Role based permissions were implemented where feasible.			
Awareness				
18	Operators/technicians have been trained/educated on not installing new software unrelated to operations and maintenance of the system (e.g., games, chat, gambling,	Not in Contract (NIC)		

19	Validated that personnel interacting with control system have completed annual cybersecurity training. (IA awareness online).	Not in Contract (NIC)		
20	Educated the operator/technicians that changes to the control system may have a cybersecurity impact and require coordination with CIO.	Not in Contract (NIC)		
Process				
21	Update Regional cyber-incident response plan (IRP) for any unique requirements associated with this control system.	Not in Contract (NIC)		
22	System logs have been reviewed and appropriate actions taken based on log content.	Not in Contract (NIC)		
23	Create and document cyber-preventative maintenance focusing on, at a minimum, the following core tasks: scanning, patching, reporting, configuration management (CM), log file analysis, and HBSS/Host Intrusion Preventions System, (HIPS).			
Connectivity				
24	Modems or other devices used for remote (off-site) access were disabled/removed.			
25	Disconnect vendor remote access.			
Physical Access				
26	Documented who has control over access to control system equipment locations (electrical, mechanical, communications rooms).	Not in Contract (NIC)		
27	Documented how CIO access to equipment locations is obtained to include after hours access.	Not in Contract (NIC)		
28	If system is located in classified area, Joint Personnel Adjudication System (JPAS) SMO code and POC are documented.	Not in Contract (NIC)		
29	Physical security of control system components was confirmed in the inventory.			
30	Ensure physical security of CS components was confirmed in the inventory and that access to CS components is based on need to know.			
31	Restrict use of unauthorized devices, such as personal mobile devices, in secure spaces.	Not in Contract (NIC)		
Hardware and Software				
32	Non-essential software has been removed (i.e. games, personal software, etc.) from any control system computers in the facility.			

_____ _____

CIO 2, NAVFAC *Date*

_____ _____

CIO 4, NAVFAC *Date*