Naval Facilities Engineering Systems Command

NAVFAC SOUTHEAST

Facility Related Control Systems (FRCS) Cybersecurity Contract Requirements

Presented by: Kevin Gaddist

Panel: Antonio Jefferson, Joe Ellis, Charlie Weaver & Keith Long

11 Jan 2024

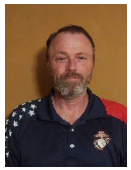
CIO Cybersecurity POCs

CYBERSECURITY PROGRAM OVERSIGHT

CIO2 CYBERSECURITY

CIO2: Joseph Ellis
Cybersecurity Division Director
joseph.p.ellis.civ@us.navy.mil

CIO21: Maria Lopez
RMF Team Lead
Risk Management Framework (RMF)
Requests for Authority-to-Operate (ATO)
maria.t.lopez.civ@us.navy.mil



CIO42: Bobby Kelley
Control Systems Support Branch Manager
AMI, SCADA, DDC, and HVAC Support
Cyber Hygiene & Continuous Monitoring Support
bobby.j.kelley.civ@us.navy.mil

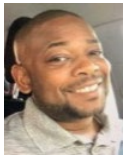
CIO: Andrea Freeman
Command Information Officer
andrea.l.freeman.civ@us.navy.mil

CIOPM: Antonio Jefferson
Cybersecurity Contracts Program Manager
Red Zone Commissioning and BOD Support
Construction and Design Contracts Review
antonio.s.jefferson2.civ@us.navy.mil

CIO43: Paddy Jackson –
Information Systems Security Engineer Team Lead
Cybersecurity Commissioning Support
Risk Management Framework (RMF) Support
paddy.o.jackson.civ@us.navy.mil

CIO4 OPERATIONAL TECHNOLOGY

CIO4: Charlie Weaver
Operation Technology Division Director
charles.r.weaver12.civ@us.navy.mil



CIO41: Kevin Gaddist
OT Enterprise Support Branch Manager
Control System Platform Enclave (CSPE)
Continuous Monitoring Support
kevin.k.gaddist.civ@us.navy.mil

CIO44: Keith Long
CyCx Team Lead
Cybersecurity Commissioning Support
Construction and Design Contracts Review
keith.d.long2.civ@us.navy.mil

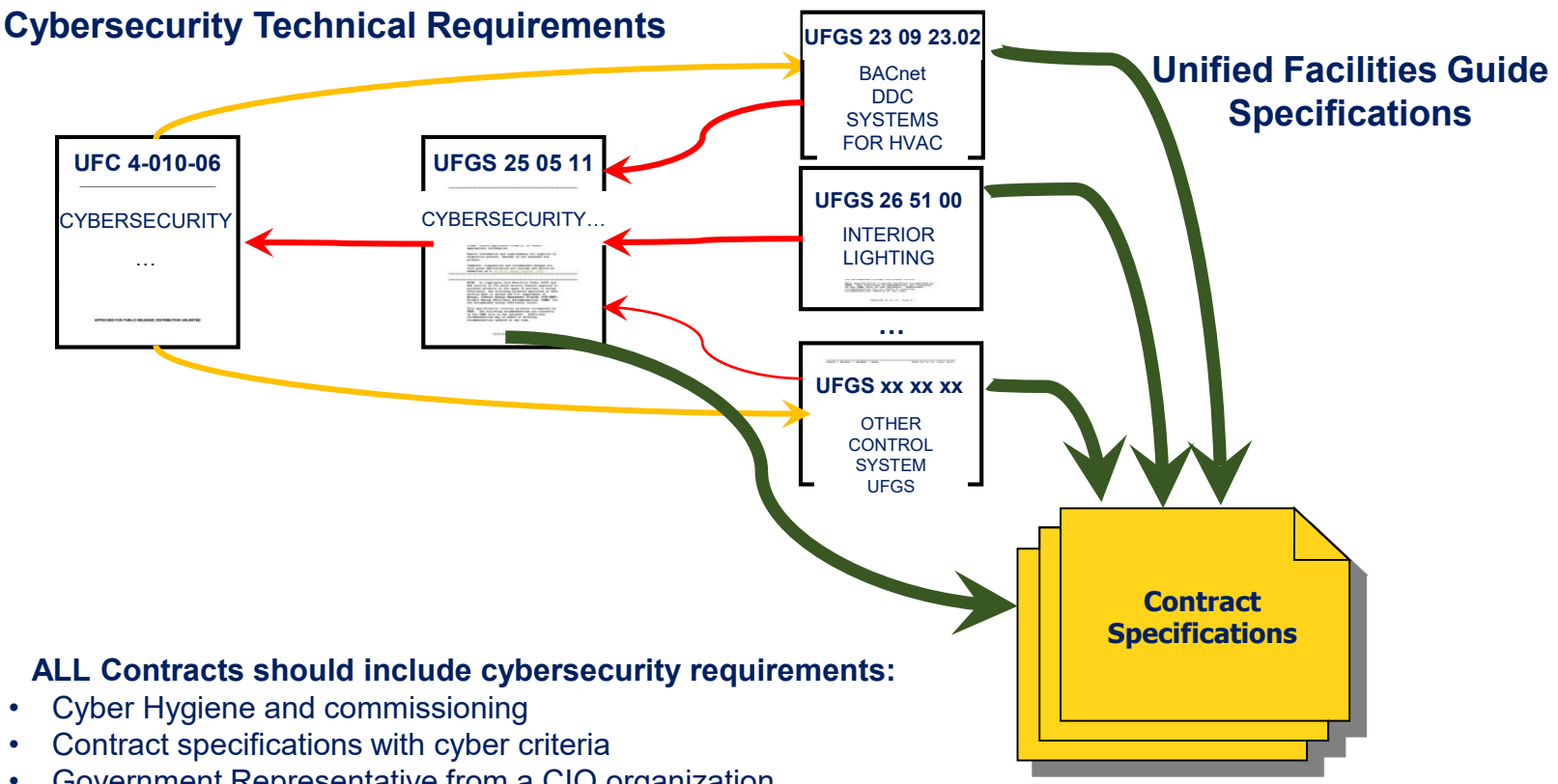
Control Systems That Require Cybersecurity

- **Building Automation Systems (BAS)**
  - Heating, Ventilation, and Air Conditioning (HVAC)
  - Lighting Control
  - Fire Protection/Life Safety
  - Utility Monitoring and Control System (UMCS)
  - Electronic Security Systems (ESS)
  - Other systems
- **Supervisory Control and Data Acquisition) (SCADA)**
- **Industrial Control Systems (ICS)**

NAVFAC Naval Facilities Engineering Systems Command NAVFAC SOUTHEAST

Guidance To Properly Secure Facility Related Control Systems (FRCS)

Unified Facilities Criteria (UFC) for Cybersecurity

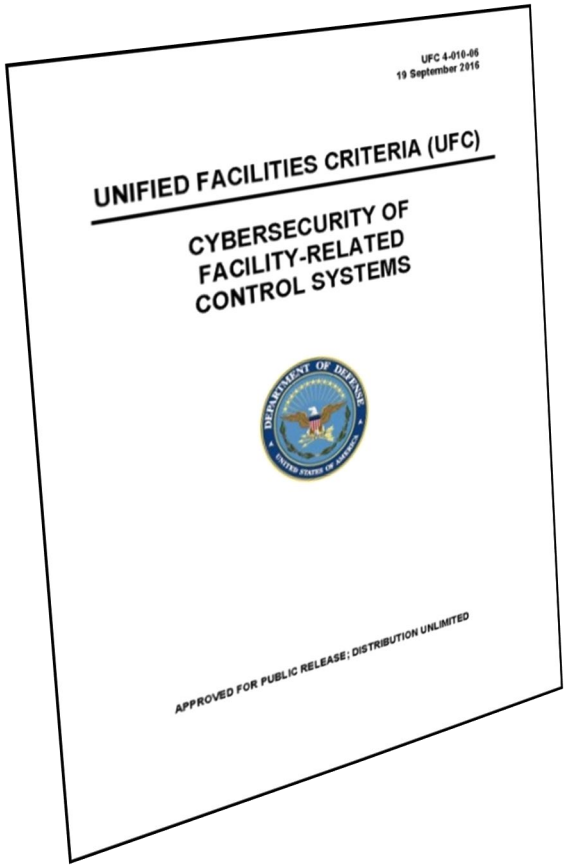


ALL Contracts should include cybersecurity requirements:

- Cyber Hygiene and commissioning
- Contract specifications with cyber criteria
- Government Representative from a CIO organization

Cybersecurity Criteria Should Be Included In Contract Specifications

Cybersecurity of Facility Related Control Systems: UFC 4-010-06



Update published 10-October-2023

Unified Facilities Criteria (UFC)

- Provides planning, design, construction, sustainment, restoration, and modernization criteria.
- Applies to the Military Departments, the Defense Agencies, and the DoD Field Activities
- Used for all DoD projects and work for other customers where appropriate

- **Integrates only a subset of Risk Management Framework (RMF) requirements for facility-related control systems**
- **Applies to all new construction and repair projects**
- **Narrows RMF Focus to design only and not system life cycle**
- **4-010-06 provides:**
  - Guidance to Designers-of-Record
  - Information intended for Designers-of-Record
  - Cyber Impact Levels of Confidentiality, Integrity, & Availability (C-I-A) Guidance for impact rating
  - Detailed guidance for LOW and MODERATE impact systems

5 Steps for Cybersecurity Design: UFC 4-010-06

- **Step 1:** Identify the Confidentiality, Integrity, and Availability (C-I-A) impact levels (LOW, MODERATE, or HIGH) to use for the control system design.
- **Step 2A:** Use the impact levels to select the proper list of controls from NIST SP 800-82.
- **Step 2B:** Create a list of relevant Control Correlation Identifiers (CCIs) based on the controls selected in Step 2A using the DoD master CCI list.
- **Step 2C:** Categorize CCIs and identify CCIs that require input from the designer or are the designer's responsibility.
- **Step 3:** Include cybersecurity requirements in the project specifications and provide input to others as required.

Design cannot proceed without the proper C-I-A Impact ratings

C-I-A Impact Ratings

Using the C-I-A impact ratings (LOW, MODERATE or HIGH) the Designer of Record (i.e. an A&E firm hired to do design work) will select security controls for the system.

- **Examples of controls are:**
  - **Access Control (AC)**
  - **Audit and Accountability (AU)**
  - **System and Communications Protection (SC)**
- **There are a total of 18 families of security controls**
- **Controls can be found in the NIST SP 800-82 and UFC 4-010-06**

ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance	PM	Program Management

Security Control Example from the UFC

Security Control ID	Security Control Name and Design Guidance
AC-2	**Account Management**: Specify what account types provide which permissions in the control system (e.g. "view only", "acknowledge alarms", "change set-points", etc.). Note that designer may need to explain these roles to the ISSM / ISSO so they can perform their DoD-defined duties under this control. Note that "accounts" (and particularly "temporary" or "emergency" accounts) likely exist at Level 4 and may or may not exist at Levels 1 or 2, depending on the control system type. (For example, many building control systems won't have user accounts at these levels, but many utility control systems do). Designer may need to explain lack of "accounts" at Levels 1 and 2. Specifications should require that account activities be audited (logged), but auditing may be limited to software applications, and require notification be supported. Note that notification (e.g. email, rollup to another system) will generally require Platform Enclave or other Level 4 and Level 5 support for actual execution.
AC-3	**Access Enforcement:** AC-3 is met by requiring the contractor to configure any control system component which has a STIG or SRG in accordance with that STIG or SRG"

Categorize & Identify the CCI's That Require Input

Can the control system do what is required in the CCI?

- CCI-000048 states that the information system display's the organization use banner
- If the control system is capable of this include it in the United Facilities Guide Specification (UFGS)
- If the control system cannot do this, lists the reasons and state that it is impractical

Table H-1 Summary of CCIs for LOW and MODERATE Impact Systems

CCI #	800-53 Control Text Indicator	Applies At Or Above Impact	Table Reference	Applicable to a Control System?
CCI-002107	AC-1 (a)	LOW	None (Non-Designer)	TRUE
CCI-002108	AC-1 (a)	LOW	None (Non-Designer)	TRUE
CCI-000001	AC-1 (a) (1)	LOW	None (Non-Designer)	TRUE
CCI-000002	AC-1 (a) (1)	LOW	None (Non-Designer)	TRUE
CCI-002106	AC-1 (a) (1)	LOW	None (Non-Designer)	TRUE
CCI-000004	AC-1 (a) (2)	LOW	None (Non-Designer)	TRUE
CCI-000005	AC-1 (a) (2)	LOW	None (Non-Designer)	TRUE
CCI-002109	AC-1 (a) (2)	LOW	None (Non-Designer)	TRUE
CCI-000003	AC-1 (b) (1)	LOW	None (Non-Designer)	TRUE
CCI-001545	AC-1(b)(1)	LOW		TRUE
CCI-000006	AC-1(b)(2)	LOW	None (Non-Designer)	TRUE
CCI-001546	AC-1(b)(2)	LOW		TRUE
CCI-002110	AC-2(a)	LOW	Table H-4 (Designer)	TRUE
CCI-002111	AC-2(a)	LOW	None (Non-Designer)	TRUE
CCI-002112	AC-2(b)	LOW	None (Non-Designer)	TRUE
CCI-000008	AC-2(c)	LOW	None (Non-Designer)	TRUE
CCI-002113	AC-2(c)	LOW	None (Non-Designer)	TRUE
CCI-002115	AC-2(d)	LOW	None (Non-Designer)	TRUE
CCI-002116	AC-2(d)	LOW	None (Non-Designer)	TRUE
CCI-002117	AC-2(d)	LOW	None (Non-Designer)	TRUE
CCI-002118	AC-2(d)	LOW	None (Non-Designer)	TRUE
CCI-002119	AC-2(d)	LOW	None (Non-Designer)	TRUE
CCI-002120	AC-2(e)	LOW	None (Non-Designer)	TRUE
CCI-000010	AC-2(e)	LOW	None (Non-Designer)	TRUE
CCI-000011	AC-2(f)	LOW	None (Non-Designer)	TRUE
CCI-002121	AC-2(f)	LOW	None (Non-Designer)	TRUE
CCI-002122	AC-2(g)	LOW	None (Non-Designer)	TRUE
CCI-002123	AC-2(h)(1)	LOW	None (Non-Designer)	TRUE
CCI-002124	AC-2(h)(2)	LOW	None (Non-Designer)	TRUE
CCI-002125	AC-2(h)(3)	LOW	None (Non-Designer)	TRUE
CCI-002126	AC-2(i)(1)	LOW	None (Non-Designer)	TRUE
CCI-002127	AC-2(i)(2)	LOW	None (Non-Designer)	TRUE
CCI-002128	AC-2(i)(3)	LOW	None (Non-Designer)	TRUE
CCI-000012	AC-2(j)	LOW	None (Non-Designer)	TRUE
CCI-001547	AC-2(j)	LOW		TRUE
CCI-002129	AC-2(k)	LOW	None (Non-Designer)	TRUE
CCI-000015	AC-2(1)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-001682	AC-2(2)	MODERATE	Table H-5 (Designer) Table H-7 (Enclave)	TRUE

Basis of Design (10-15%)

At the Basis of Design (10-15% design) submittal, or the equivalent submittal step for projects not incorporating a Basis of Design submittal, provide the following items:

- **System Description:** A brief functional description of the system.
- **CIA Impact Level:** The C-I-A impact level for the control system and whether it was provided by the Service, or was determined using one of the courses of action described in CHAPTER 3 for when impact ratings aren't provided. If using the methods discussed in APPENDIX D provide a narrative documenting how the impact rating was determined.
- **Starting Security Control Set and Tailoring Recommendation:** A list of the security controls generated during Step 2A along with recommendations and justifications for further tailoring of the security control set.
- **Network Connectivity Description:** A general description of expected network connectivity type, such as stand-alone, closed restricted network, dedicated transport, or shared transport.
- **System Connections:** Planned, expected, or required connections to other systems (if any).

Concept Design (30-35%)

At the Concept Design (30-35% design) submittal, or the equivalent submittal step for projects not incorporating a Concept Design submittal, *provide a list of the CCIs resulting from the approved tailored security control list (Step 2B) or provided by the Service*, and an initial classification for each CCI (Step 2C).

Interim Design (50-65%)

At the Interim Design (50-65% design) submittal, or the equivalent submittal step for projects not incorporating an Interim Design submittal, provide the following items:

- **CCI List**: The recommended format for this list is to use the format of the tables in APPENDIX G with the addition of a column to document the required information. In addition to any other required formats, provide the CCI list in a format compatible with Microsoft Excel. The list must include the following items:
  - The final classification (Designer, etc..) of each CCI (Step 2C).
  - For each CCI categorized as designer and addressed in the design, include:
    - Identification where and why the standard CCI requirements cannot be incorporated into the design (identified in Step 3), description of what requirements will be incorporated instead, and an explanation of the changes.
    - Documentation of how the CCI has been incorporated into the control system design (Step 3), including specification or drawing references. If there are specific changes from standard requirements, or multiple options available, document these changes or options.
    - For each CCI categorized as designer due to requiring information be provided (Step 3), provide the relevant information for use by others.
- **Redlined Specifications and Drawings:** Draft specifications based on UFGS 25 05 11 with appropriate tailoring for system type and impact rating and edited for project requirements, and any relevant drawings or other attachments when requirements have been incorporated into drawings or other attachments.
- **Riser Diagrams**: One-line/riser diagram showing concept architecture and major components.
- **System Connections:** A document either indicating no network connections to other systems will exist or describing the network connections to other systems. For system connections include a description of the other system, the nature and purpose of the connection, and all protocols used by the communication interface.

Final Design (Un-reviewed 100%)

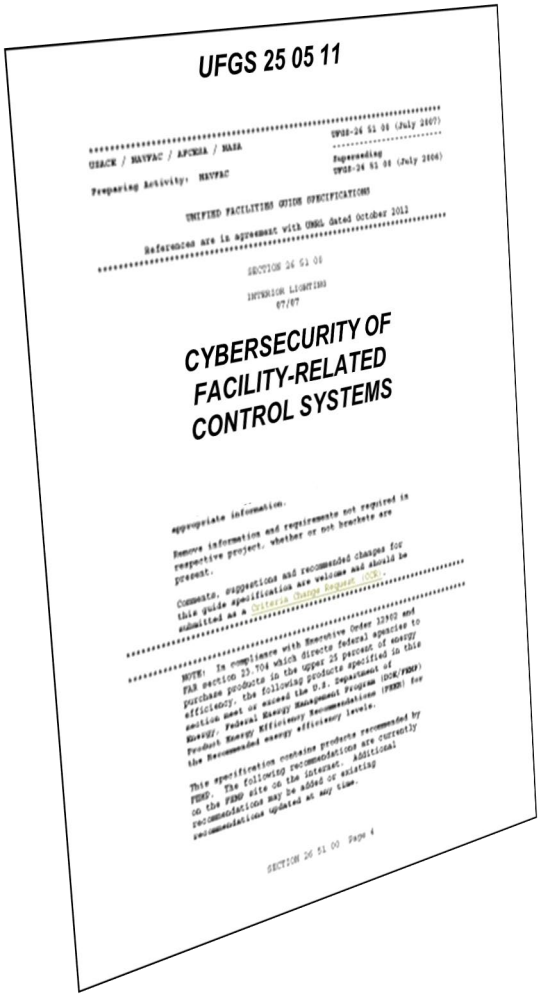
At the Final Design (Un-reviewed 100% design) submittal, or the equivalent submittal step for projects not incorporating a Final Design submittal, *provide all items from the Interim Design (50-65%) with updated Final Design information.*

NAVFAC Naval Facilities Engineering Systems Command NAVFAC SOUTHEAST

Issued for Construction (Reviewed 100%)

At the Issued for Construction (Reviewed 100% design) submittal, or the equivalent submittal step for projects not incorporating an Issued for Construction submittal, provide all items from the Final Design (Un-reviewed 100%) with updated Issued for Construction information.

Cybersecurity of Facility Related Control Systems: UFGS 25 05 11


UFGS 25 05 11

CYBERSECURITY OF FACILITY-RELATED CONTROL SYSTEMS

- Update published August 2023
  - Whole Building Design Guide (www.wbdg.org)
- Consolidated all cybersecurity submittals into one specification
- Includes requirements to submit for contractual fulfillment by implementing cybersecurity into facility related controlled systems construction projects
- Requires security control submittals to be properly answered

NAVFAC FRCS CyCx Checklist Example: Control Implementation Assessment

NAVFAC FRCS Cybersecurity Commissioning (CyCx) Checklist

Project or Work Order Number:	
Control System or Device/Component (Choose one):	
Control System or Device/Component Name:	
Date:	

Read instruction tab before completing this checklist. Contractor is to complete this checklist for each control system and/or component. These devices will range between Levels 2 - 5 of the UFC 04-01-06 Control System Architecture. ***NOTE: If each device type is identical and configured the same, only one sheet required.***

Task ID	Requirement	Reference	Status	Comments
	Contractor/Vendor			
C1	Have all unused accounts been deleted from control system?	AC-2		
C2	Have all shared credentials/accounts utilized on the control system been approved by the government. If not, provide explanation in the comments.	AC-2		
C3	Have all control system accounts been modified to the concept of least privileged; leaving only authorized user and services access required to meet the mission of the system?	AC-6		
C4	Are there user initiated methods and/or mechanism to prevent unauthorized access to the control system when left unattended?	AC-11		
C5	Has all remote access been approved by the government?	AC-17		
C6	Are all control system wireless network access configured with to the DoD approved encryption standards? If not, provide explanation in comments?	AC-18		
C7	Have control system logs have been reviewed and appropriate actions taken based on log content (i.e. alarms)?	AU-1		
C8	Has the inventory of all physical devices and systems been documented on a control system inventory and approved by the government?	CM-8		
C9	Has the inventory of all software and software licenses been documented and approved by the government?	CM-8		
C10	Have all default passwords been changed to meet the DoD password standards or set to the maximum strength allowable by the operating system or firmware?	IA-5		
C11	Are all physical access points to the control system and its components installed where monitored physical access authorization controls are in place (i.e., CCTV, alarms, guards) or is properly secured (i.e., behind a locked door or enclosure)? If not, provide explanation in comments.	PE-3, PE-6		
C12	Does the control system have long-term alternate power supply in the event of an extended loss of the primary power source?	PE-11		
C13	Have all control system parts and replacement components been verified as genuine and not been altered?	SA-12		
C14	Has government approved installation of any components and software approaching or at end of life support?	SA-22		
C15	Does the control system fail to a secure state in an event of a failure during system initialization, shutdown, and aborts?	SC-24		
C16	Are all non-essential or unrequested functionalities, connection ports and input/output devices physically disabled or removed?	SC-41		
	Government Use Only			
G1	All privilege user have an approved Navy System Access Authorization Request (SAAR-N) on file documenting a proper background investigation and completed privileged access agreement?	AC-6(5)		
G2	All operator/technician(s) have an approved Navy System Access Authorization Request (SAAR-N) on file documenting completion of annual Cyber Awareness Training.	AT-2		
G3	Has a Continuous Monitoring plan been documented, and if so, has that Plan been implemented which focuses on, at a minimum, the following core tasks: POA&M updates, patching, reporting, configuration management (CM), log file analysis, account management, firmware updates? (To include scanning when possible/applicable)	CA-7		
G4	Have the operator/technician(s) been informed that changes to the control system baseline may have a cybersecurity impact and require coordination with CIO/N6/System Owner.	CM-2		
G5	Has the Incident Response Plan (IRP) applicable to this control system been updated for any unique requirements associated with this control system? If so, provide explanation in the comments.	IR-1		
G6	Has the Physical Security Officer and after-hours point of contract of the control system space been documented? If not, document in the comments.	MA-5		

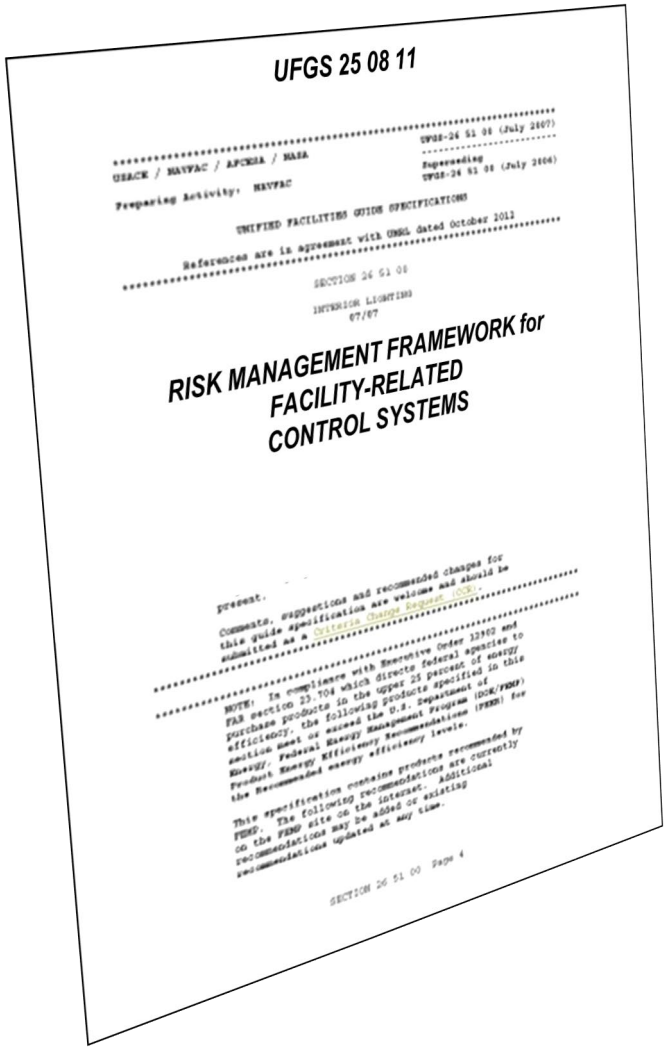
NAVFAC FRCS Cybersecurity Commissioning (CyCx) Checklist

Project or Work Order Number:	P426
Control System or Device/Component (Choose one):	Control System
Control System or Device/Component Name:	LCS Facility DDC
Date:	Monday, May 16, 2022

Read instruction tab before completing this checklist. Contractor is to complete this checklist for each control system and/or component. These devices will range between Levels 2 - 5 of the UFC 04-01-06 Control System Architecture. ***NOTE: If each device type is identical and configured the same, only one sheet required.***

Task ID	Requirement	Reference	Status	Comments
	Contractor/Vendor			
C1	Have all unused accounts been deleted from control system?	AC-2	Compliant	No unused account present.
C2	Have all shared credentials/accounts utilized on the control system been approved by the government. If not, provide explanation in the comments.	AC-2	Compliant	There are no shared accounts associated with the system
C3	Have all control system accounts been modified to the concept of least privileged; leaving only authorized user and services access required to meet the mission of the system?	AC-6	Compliant	At this time there are only one account for administrative purposes
C4	Are there user initiated methods and/or mechanism to prevent unauthorized access to the control system when left unattended?	AC-11	Not Applicable	Requirement will be re-assessed for update to checklist.
C5	Has all remote access been approved by the government?	AC-17	Compliant	There is remote access connectivity
C6	Are all control system wireless network access configured with to the DoD approved encryption standards? If not, provide explanation in comments?	AC-18	Not Applicable	Wireless mechanism will be physically removed from JACE.
C7	Have control system logs have been reviewed and appropriate actions taken based on log content (i.e. alarms)?	AU-1	Not Applicable	N/A at this time until fully operational
C8	Has the inventory of all physical devices and systems been documented on a control system inventory and approved by the government?	CM-8	Compliant	
C9	Has the inventory of all software and software licenses been documented and approved by the government?	CM-8	Compliant	
C10	Have all default passwords been changed to meet the DoD password standards or set to the maximum strength allowable by the operating system or firmware?	IA-5	Not Applicable	At this time this security controls has not been implemented until full turnover.
C11	Are all physical access points to the control system and its components installed where monitored physical access authorization controls are in place (i.e., CCTV, alarms, guards) or is properly secured (i.e., behind a locked door or enclosure)? If not, provide explanation in comments.	PE-3, PE-6	Compliant	CAC enabled readers for door locks are installed throughout the facility
C12	Does the control system have long-term alternate power supply in the event of an extended loss of the primary power source?	PE-11	Not Applicable	CIO will determine if building generator will power building PLCs and other level 0 and 1 device.
C13	Have all control system parts and replacement components been verified as genuine and not been altered?	SA-12	Not Applicable	Requirement will be re-assessed for update to checklist.
C14	Has government approved installation of any components and software approaching or at end of life support?	SA-22	Not Applicable	End of life is 3 years or more away.
C15	Does the control system fail to a secure state in an event of a failure during system initialization, shutdown, and aborts?	SC-24	Not Applicable	Besides for the laptop all other devices are programmable controllers
C16	Are all non-essential or unrequested functionalities, connection ports and input/output devices physically disabled or removed?	SC-41	Compliant	There are no non-essential port connections
	Government Use Only			
G1	All privilege user have an approved Navy System Access Authorization Request (SAAR-N) on file documenting a proper background investigation and completed privileged access agreement?	AC-6(5)	Not Applicable	Only 1 contractor account present. Upon turnover, contractor account will removed and SAARs verified before account creation.
G2	All operator/technician(s) have an approved Navy System Access Authorization Request (SAAR-N) on file documenting completion of annual Cyber Awareness Training.	AT-2	Not Applicable	Only 1 contractor account present. Upon turnover, contractor account will removed and SAARs verified before account creation.
G3	Has a Continuous Monitoring plan been documented, and if so, has that Plan been implemented which focuses on, at a minimum, the following core tasks: POA&M updates, patching, reporting, configuration management (CM), log file analysis, account management, firmware updates? (To include scanning when possible/applicable)	CA-7	Not Applicable	This was just an assessment of a system without an ATO contract.
G4	Have the operator/technician(s) been informed that changes to the control system baseline may have a cybersecurity impact and require coordination with CIO/N6/System Owner.	CM-2	Compliant	CIO provided change management training to BOSC COR and System Owner.
G5	Has the Incident Response Plan (IRP) applicable to this control system been updated for any unique requirements associated with this control system? If so, provide explanation in the comments.	IR-1	Compliant	System will follow NS Mayport IRP and follow NAVFAC SE CCIR.
G6	Has the Physical Security Officer and after-hours point of contract of the control system space been documented? If not, document in the comments.	MA-5	Compliant	Information was collected by the CIO2 OT ISSM

RMF of FRCS: UFGS 25 08 11


UFGS 25 08 11

USACE / NAVFAC / AFCEEA / NASA

UFGS-26 51 08 (July 2007)

Preparing Activity: NAVFAC

Superseding
UFGS-26 51 08 (July 2006)

UNIFIED FACILITIES GUIDE SPECIFICATIONS

References are in agreement with UMCL dated October 2012

SECTION 26 51 08

INTERIOR LIGHTING
07/07

RISK MANAGEMENT FRAMEWORK for
FACILITY-RELATED
CONTROL SYSTEMS

present.

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

NOTE: In compliance with Executive Order 13693 and FAR section 23.704 which directs federal agencies to purchase products in the upper 25 percent of energy efficiency, the following products specified in this section meet or exceed the U.S. Department of Energy, Federal Energy Management Program (DOE/FEMP) Product Energy Efficiency Recommendations (PEER) for the Recommended energy efficiency levels.

This specification contains products recommended by FEMP. The following recommendations are currently on the FEMP site on the internet. Additional recommendations may be added or existing recommendations updated at any time.

SECTION 26 51 00 Page 4

- **Consolidated contract requirements for RMF of FRCS**
- **Revision published September 2020**
  - Document to support in obtaining an Authority to Operate
- **Includes requirements to submit for contractual fulfillment by implementing RMF cybersecurity into facility related controlled systems construction projects**

RMF of FRCS: UFGS 25 08 11

- Adds a cybersecurity security professional to the contractor team
- Provides translation of submittals into RMF artifacts
- Requires the contractor to have Enterprise Mission Assurance Support Service (eMASS) access and execute work inside eMASS
- Requires the government to provide the contractor with a CAC card for eMASS access
- Used in conjunction with UFGS 25 05 11 to enhance the cybersecurity service requirements of the contractor

This tool can be added to projects requiring eMASS support such as Assess Only Package and Authority to Operate

Frequently Asked Questions

1. **What is required to be Trade Agreement Act (TAA) compliant? For TAA compliance, a product must either be made in the United States or a designated country, or it must have undergone a significant change in form, fit, or function in one of these countries.**
   - https://www.gsa.gov/buy-through-us/purchasing-programs/multiple-award-schedule/help-with-mas-contracts-to-sell-to-government/roadmap-to-get-a-mas-contract/readiness-assessment-for-mas-offerors/look-up-trade-agreements-actdesignated-countries
   - https://www.acquisition.gov/far/subpart-25.4
   - https://www.acquisition.gov/far/52.225-5

2. **Is there additional Contract Compliance information available?**
   - https://vsc.gsa.gov/vsc/app-content-viewer/section/132#Trade%20Agreement%20Act%20(TAA)%20Compliance

3. **Is there an Approved Product List available?**
   - https://www.cisa.gov/resources-tools/programs/continuous-diagnostics-and-mitigation-cdm-program/program-approved-products-list-apl
   - https://aplits.disa.mil/processAPList.action

4. **Where is the NIST Special Publication SP 800-82r3 Guide to OT Security located?**
   - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf