Naval Facilities Engineering Systems Command

NAVFAC SOUTHEAST

Facility Related Control Systems (FRCS) Cybersecurity Contract Requirements

Presented by: Antonio Jefferson

Panel: Andrea Freeman, Joseph Ellis, Keith Long

09 December 2024

CIO Cybersecurity POCs

CYBERSECURITY PROGRAM OVERSIGHT

CIO: Andrea Freeman
Command Information Officer
904-542-4191

CIO2 CYBERSECURITY

CIO2: Joseph Ellis
Cybersecurity Division Director
904-542-5839

CIO21: Maria Lopez
RMF Team Lead
Risk Management Framework (RMF)
Requests for Authority-to-Operate (ATO)
904-546-9060

CIO42: Bobby Kelley
Control Systems Support Branch Manager
AMI, SCADA, DDC, and HVAC Support
Cyber Hygiene & Continuous Monitoring Support
904-542-2490

CIOPM: Antonio Jefferson
Cybersecurity Program Manager
Red Zone/Cybersecurity Commissioning
Construction and Design Contracts Review
904-546-9056

CIO43: Paddy Jackson
Information Systems Security Engineer Team Lead
Cybersecurity Commissioning Support
Risk Management Framework (RMF) Support
904-542-5488

CIO4 OPERATIONAL TECHNOLOGY

CIO4: : Kevin Gaddist
Acting Operation Technology Division Director
904-542-8495

CIOC2: Joseph Ellis
Defensive Cybersecurity Operations
Protect Systems and Networks from Cyber Threats
Analyze Cyber Threats and Vulnerabilities
904-542-5839

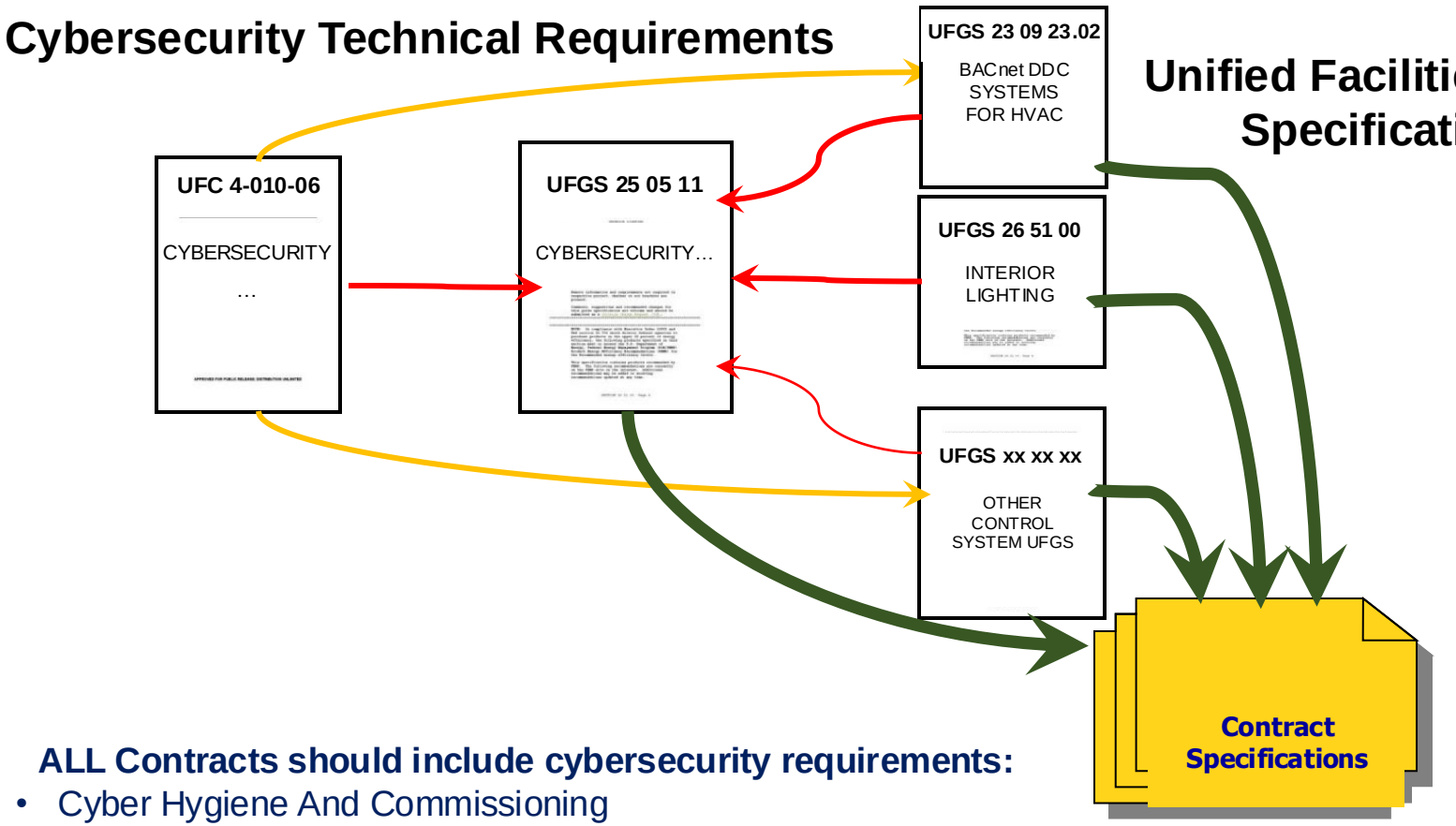
CIO44: Keith Long
CyCx Team Lead
Cybersecurity Commissioning Support
Construction and Design Contracts Review
904-542-8434

Control Systems That Require Cybersecurity

- **Industrial Control Systems (ICS)**
  - **Supervisory Control and Data Acquisition (SCADA) systems**: Used to control assets that are spread out geographically
  - **Power Generation Systems -** components that convert energy from a source like fossil fuels, wind, solar, or water into electricity
  - **Programmable Logic Controllers (PLCs):** Used to control localized processes
  - **Field Devices:** Receive supervisory commands from remote stations to control local operations
- **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**

Guidance To Properly Secure Facility Related Control Systems (FRCS)

Unified Facilities Criteria (UFC) for Cybersecurity

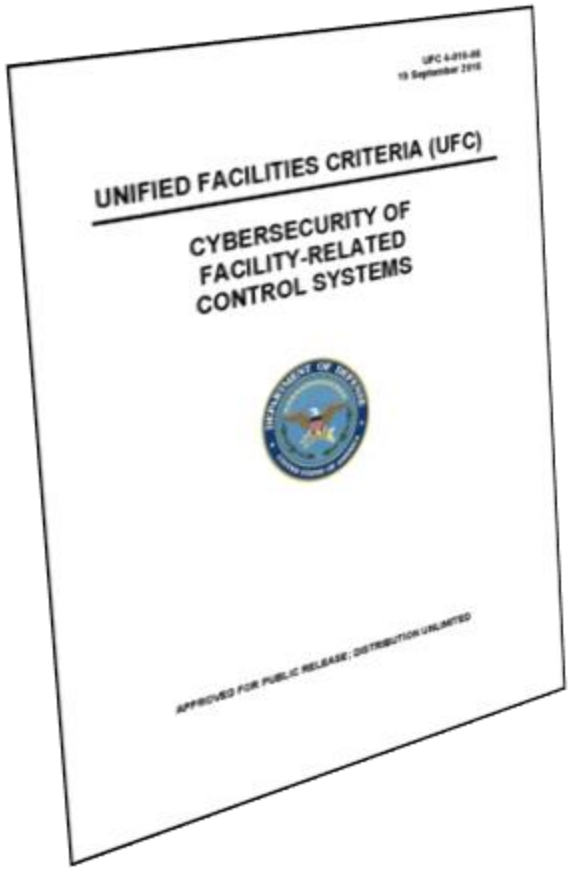


ALL Contracts should include cybersecurity requirements:

- Cyber Hygiene And Commissioning
- Contract Specifications With Cyber Criteria
- Government Representative From A CIO Department/Organization

Cybersecurity Criteria Should Be Included In Contract Specifications

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



UPDATE PUBLISHED 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 should not 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

Example of a Security Control 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 CCIs 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

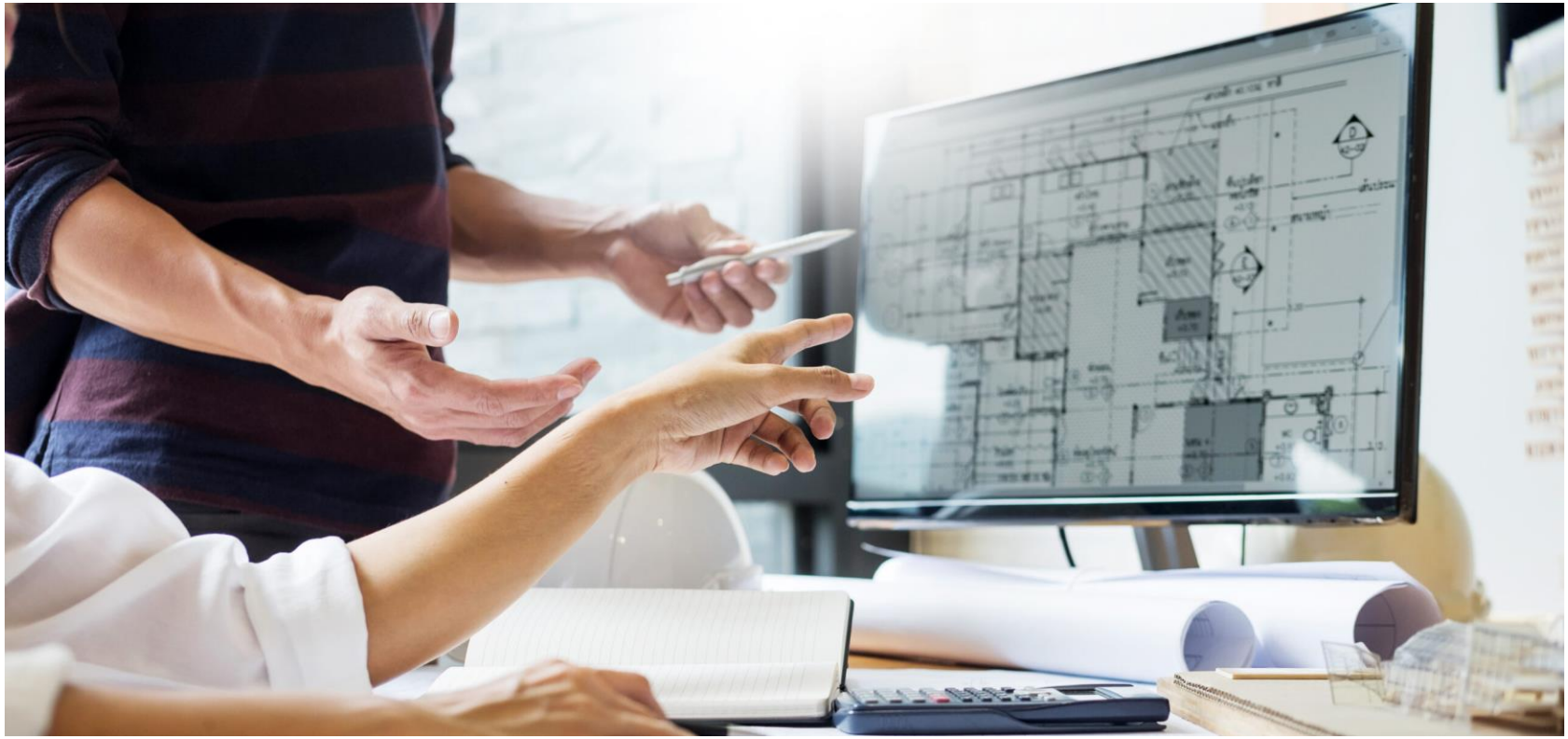
Basis of Design (10-15%)

The is the Basis of Design (10-15% design) submittal, or the equivalent submittal step for a Design Build or Design Bid Build contract. The following items are provided:

- **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%)

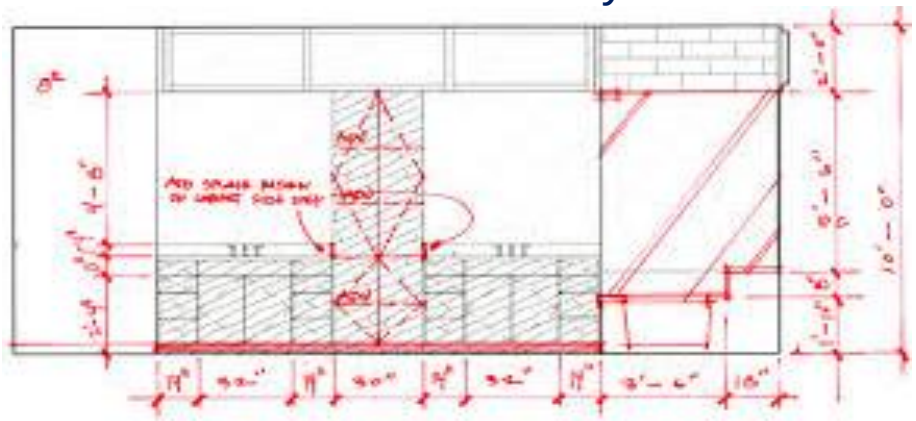
The Concept Design (30-35% design) submittal, provides a list of the Common Control Identifiers (CCIs) resulting from the approved tailored security control list created by the Designer of Record (DOR).

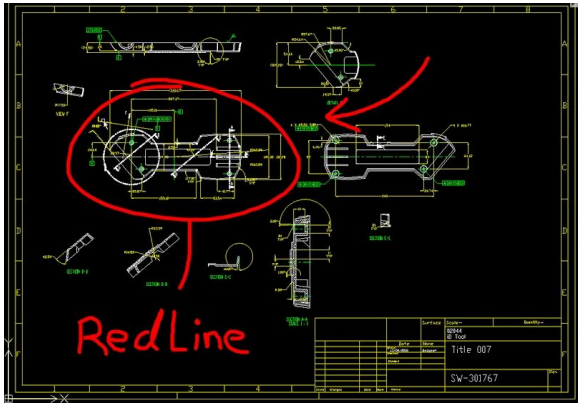


Interim Design (50-65%)

The Interim Design (50-65% design) submittal provides the following items:

- **CCI List**: Must include the final classification of each CCI:
- **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.
- **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





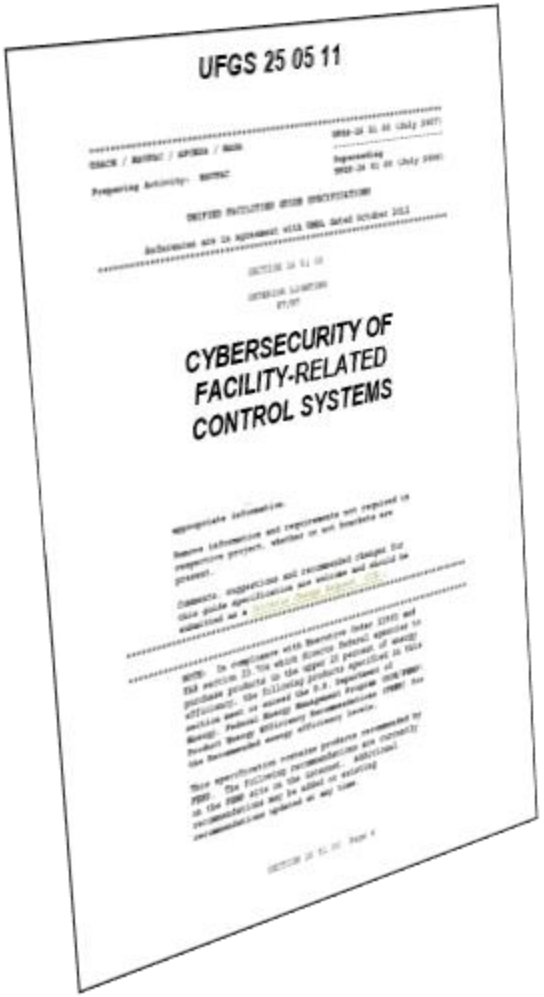
Final Design (Un-reviewed 100%)

The Final Design (Un-reviewed 100% design) submittal, *provides all items from the Interim Design (50-65%) with updated Final Design information.*

Issued for Construction (Reviewed 100%)

The Issued for Construction (Reviewed 100% design) submittal, provides 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

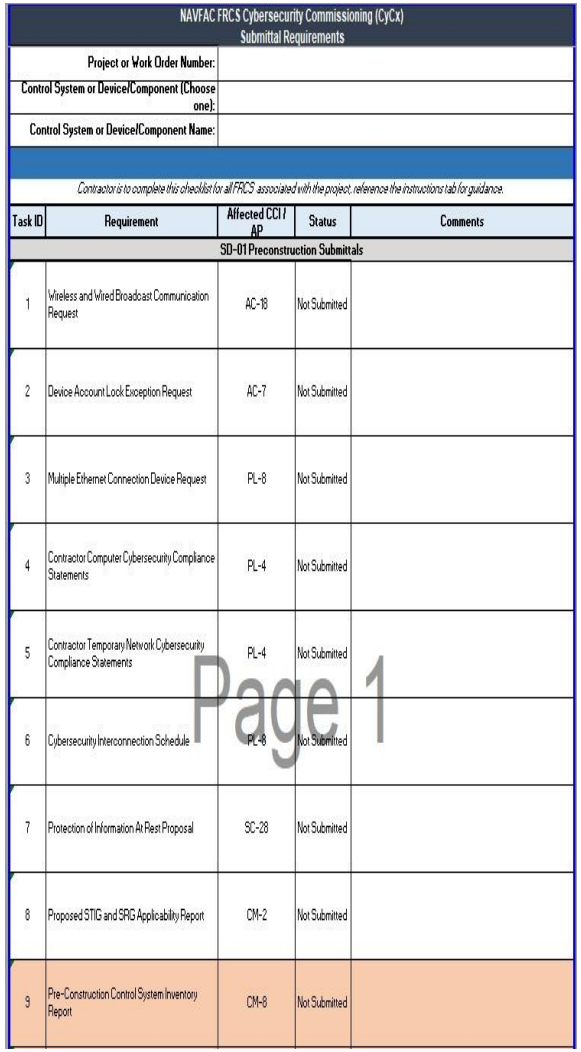

UFGS 25 05 11

CYBERSECURITY OF FACILITY-RELATED CONTROL SYSTEMS

UPDATE REVISION PUBLISHED AUGUST 2024

- Whole Building Design Guide (www.wbdg.org)
- Consolidates 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

FRCS CyCx Checklist Example: Other Requirements (Submittals)



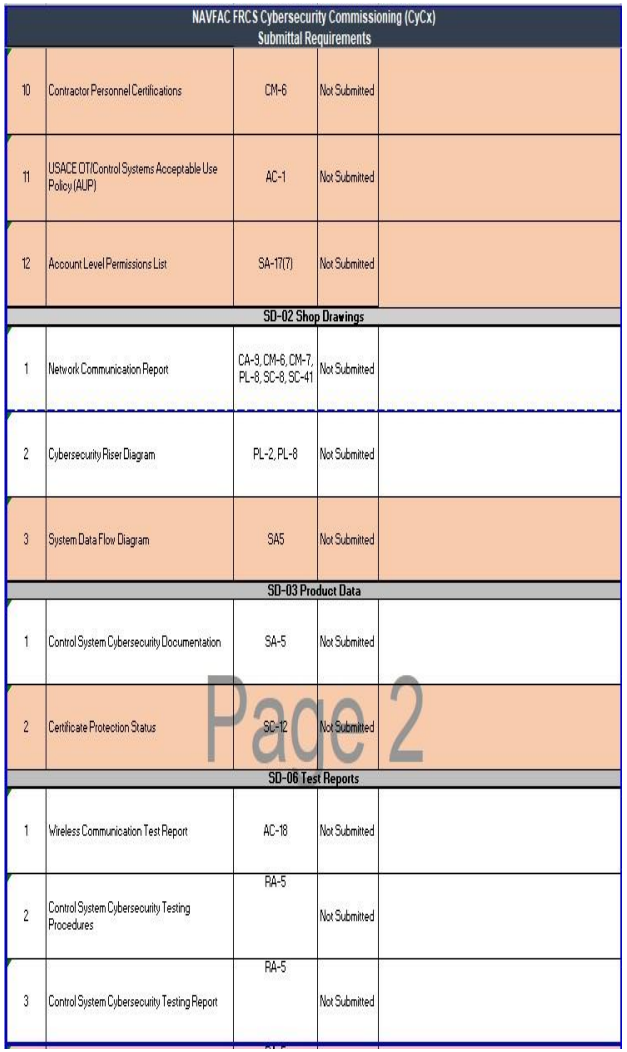
NAVFAC FRCS Cybersecurity Commissioning (CyCx)
Submittal Requirements

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

Contractor is to complete this checklist for all FRCS associated with the project, reference the instructions tab for guidance.

Task ID	Requirement	Affected CCI / AP	Status	Comments
SD-01 Preconstruction Submittals				
1	Wireless and Wired Broadcast Communication Request	AC-18	Not Submitted	
2	Device Account Lock Exception Request	AC-7	Not Submitted	
3	Multiple Ethernet Connection Device Request	PL-8	Not Submitted	
4	Contractor Computer Cybersecurity Compliance Statements	PL-4	Not Submitted	
5	Contractor Temporary Network Cybersecurity Compliance Statements	PL-4	Not Submitted	
6	Cybersecurity Interconnection Schedule	PL-8	Not Submitted	
7	Protection of Information At Rest Proposal	SC-28	Not Submitted	
8	Proposed STIG and SRG Applicability Report	CM-2	Not Submitted	
9	Pre-Construction Control System Inventory Report	CM-8	Not Submitted	

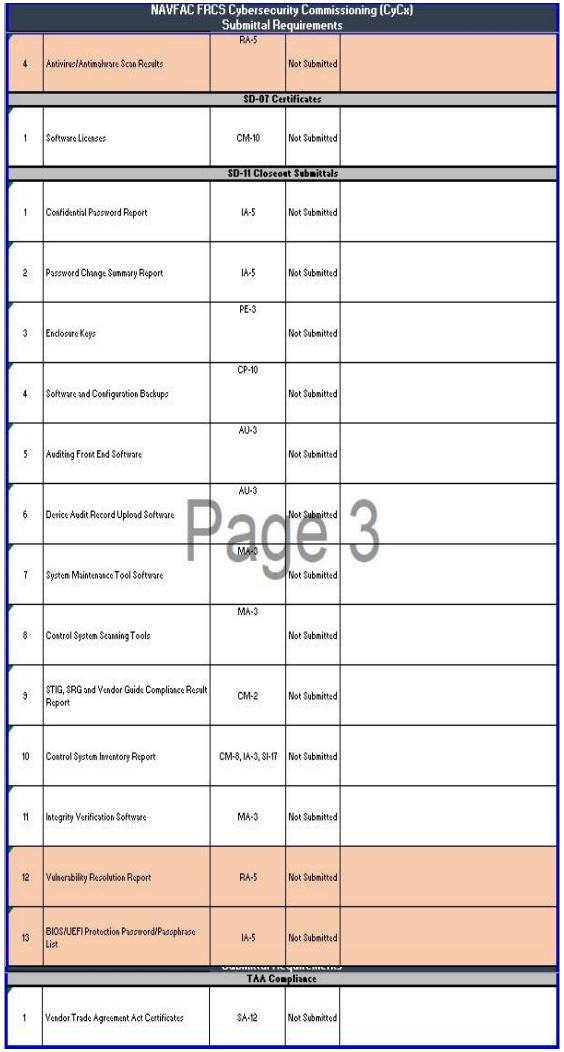
Page 1



NAVFAC FRCS Cybersecurity Commissioning (CyCx)
Submittal Requirements

10	Contractor Personnel Certifications	CM-6	Not Submitted	
11	USACE OT/Control Systems Acceptable Use Policy (AUP)	AC-1	Not Submitted	
12	Account Level Permissions List	SA-17(7)	Not Submitted	
SD-02 Shop Drawings				
1	Network Communication Report	CA-9, CM-6, CM-7, PL-8, SC-8, SC-41	Not Submitted	
2	Cybersecurity Riser Diagram	PL-2, PL-8	Not Submitted	
3	System Data Flow Diagram	SA5	Not Submitted	
SD-03 Product Data				
1	Control System Cybersecurity Documentation	SA-5	Not Submitted	
2	Certificate Protection Status	SC-12	Not Submitted	
SD-06 Test Reports				
1	Wireless Communication Test Report	AC-18	Not Submitted	
2	Control System Cybersecurity Testing Procedures	RA-5	Not Submitted	
3	Control System Cybersecurity Testing Report	RA-5	Not Submitted	

Page 2

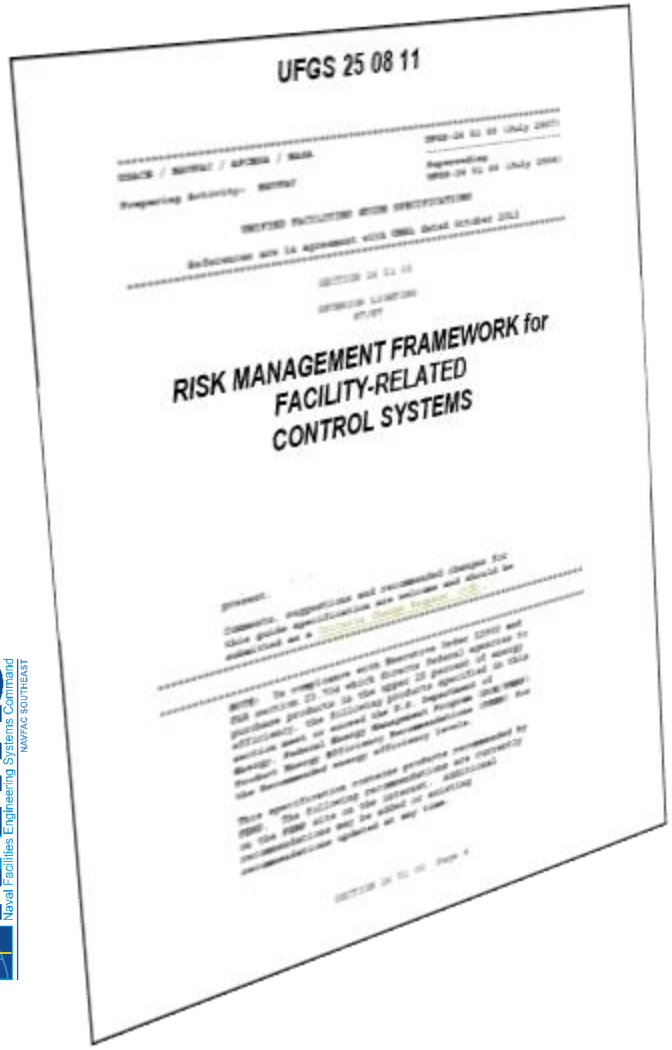


NAVFAC FRCS Cybersecurity Commissioning (CyCx)
Submittal Requirements

4	Antivirus/Antimalware Scan Results	RA-5	Not Submitted	
SD-07 Certificates				
1	Software Licenses	CM-10	Not Submitted	
SD-11 Closeout Submittals				
1	Confidential Password Report	IA-5	Not Submitted	
2	Password Change Summary Report	IA-5	Not Submitted	
3	Enclosure Keys	PE-3	Not Submitted	
4	Software and Configuration Backups	CP-10	Not Submitted	
5	Auditing Front End Software	AU-3	Not Submitted	
6	Device Audit Record Upload Software	AU-3	Not Submitted	
7	System Maintenance Tool Software	MA-3	Not Submitted	
8	Control System Scanning Tools	MA-3	Not Submitted	
9	STIG, SRG and Vendor Guide Compliance Result Report	CM-2	Not Submitted	
10	Control System Inventory Report	CM-8, IA-3, SI-17	Not Submitted	
11	Integrity Verification Software	MA-3	Not Submitted	
12	Vulnerability Resolution Report	RA-5	Not Submitted	
13	BIOS/UEFI Protection Password/Passphrase List	IA-5	Not Submitted	
TAA Compliance				
1	Vendor Trade Agreement Act Certificates	SA-12	Not Submitted	

Page 3

RMF of FRCS: UFGS 25 08 11



PUBLISHED NOVEMBER 2020

- Whole Building Design Guide (www.wbdg.org)

- **Provides RMF contract requirements for FRCS**
  This guide specification covers the Navy requirements to support the Risk Management Framework (RMF) Authority to Operate (ATO) Process for Facility-Related Control Systems.

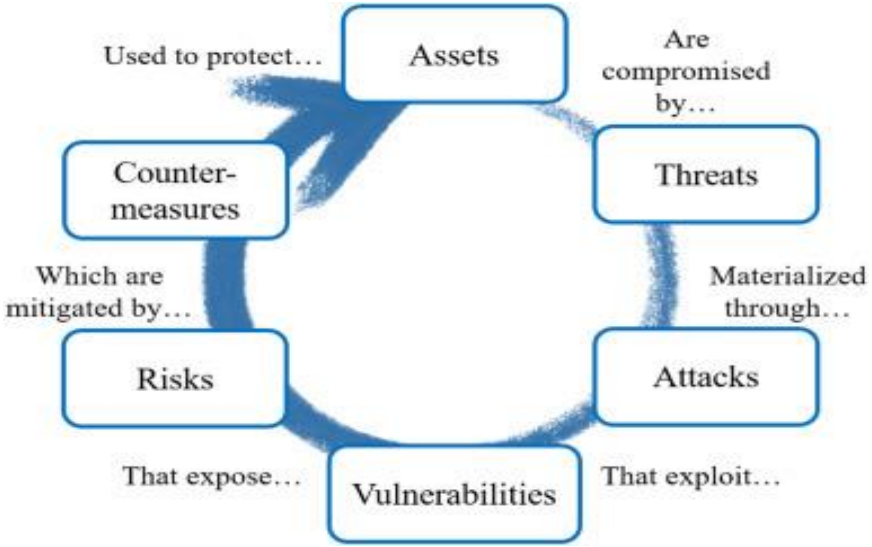
- **Includes requirements to submit for contractual fulfillment by implementing RMF cybersecurity into facility related controlled systems construction projects**

- **Only use this specification on control systems which are obtaining a new ATO.**

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 for an 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?** YES
   - https://vsc.gsa.gov/vsc/app-content-viewer/section/132#Trade%20Agreement%20Act%20(TAA)%20Compliance

3. **Is there an Approved Product List available?** YES
   - 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

Questions?