

The New UFC 4-010-06 of 2023: A Practical Breakdown

Moderator: Lori Jackson, President, White Raven Security

Speaker: F. Charlene Watson, HDR, Inc.

GICSP, CISSP, CISM, CRISC, CEH

May 14, 2024, 1:30 p.m.



MODERATOR



Lori Jackson
White Raven Security
President

Fun Facts

- I am a soccer fanatic
- I have 7 children
- My favorite dessert is cheesecake

MAY 14-16, 2024
ORLANDO, FL

OPERATION:
COLLABORATION

SAME SAMEJETC.ORG



 **conferences i/o**



or browse to
jetc.cnf.io

This is an interactive session.
To participate, use your mobile device:
jetc.cnf.io
Or scan the QR Code

- Find the session.
- The presenter will unlock the poll(s) during the presentation.
- Please complete a brief Evaluation Survey at the end of the session.

MAY 14-16, 2024
ORLANDO, FL

OPERATION:
COLLABORATION

SAME SAMEJETC.ORG

HOUSEKEEPING ITEMS

Take Note of Exits

Silence Your Mobile Devices

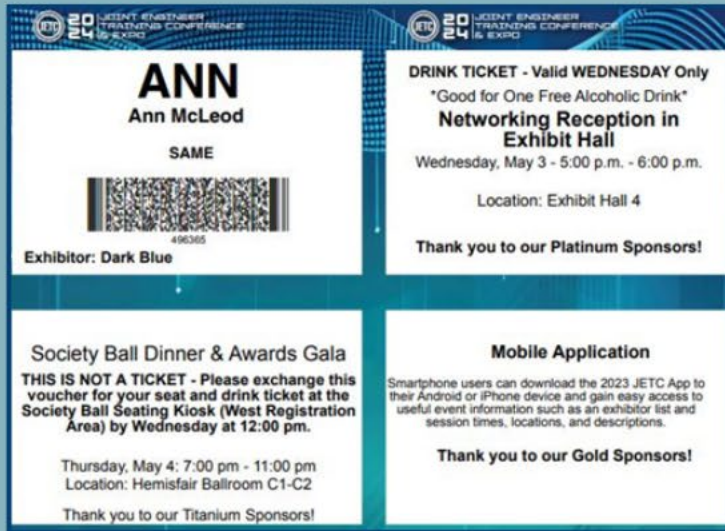
Presentations and Audio Recordings will be available in the Attendee Service Center until August 30, 2024

Download your PDH record in the Attendee Service Center before August 30, 2024



Opening Reception at Universal CityWalk

(Minimum age 18 - No Children)



Bring Your Name Badge
with Drink Tickets)
+ Your ID



Get Your Wrist Band
TODAY at the
Registration Help Desk
or SAME Booth



Buses depart Gaylord
& Caribe Royale,
beginning at 6:00 p.m.



Thank You to our Education Session Sponsors



Live Content Slide

Poll: Let's see who is in the audience...who do you represent?



SPEAKER



F. Charlene Watson

HDR, Inc.

Senior Cybersecurity Controls System
Specialist | OT Cybersecurity

Fun Facts

- I love My Little Pony
- I do not like dogs
- I was a bar bouncer

MAY 14-16, 2024
ORLANDO, FL

OPERATION:
COLLABORATION

SAME SAMEJETC.ORG

DISCLAIMER

The content of this curricula has been compiled with meticulous care. However, no presenter, company, or government entity can assume any liability nor is the

Presenter under any obligation to monitor any requirements, (e.g., licensure, regulatory, legally, or otherwise) for engineering or architecture – that falls on the licensee and/or A-E entity, Business Enterprise or Professional to monitor.

Live Content Slide

Poll: What is the title of UFC 4-010-06?

OBJECTIVES

Objective 1: Analysis of What to Include in RFPs. HINT: the UFC does NOT execute the Risk Management Framework & Does NOT Provide an ATO

Objective 2: Practical Summary of Potential Costs to PCRs, PDRs, DBs, and DBBs

Objective 3: Deep Dive Analysis of Chapter 5, Section 5-4 "REQUIREMENTS BY DESIGN PHASE"

Objective 4: Review of the new Appendix D, CONSIDERATIONS IN DETERMINATION OF CONTROL SYSTEM IMPACT RATINGS and what this means for the C-I-A Impact Ratings

What to Include in RFPs

HINT: The UFC does NOT execute the Risk Management Framework & and does NOT provide an ATO



2024

JOINT ENGINEER
TRAINING CONFERENCE
& EXPO

SAMEJETC.ORG



[PSAMENATIONAL](https://www.facebook.com/PSAMENATIONAL)



[PSAME_NATIONAL](https://twitter.com/PSAME_NATIONAL) | [#SAMEJETC24](https://twitter.com/SAMEJETC24)



["SOCIETY OF AMERICAN MILITARY ENGINEERS"](https://www.linkedin.com/company/society-of-american-military-engineers)

Count the Cost

- CYBERSECURITY DESIGN TYPICALLY FAILS BECAUSE BOTH CLIENTS AND A-ES STRUGGLE TO ACCURATELY “COUNT THE COSTS” OF CYBERSECURITY DESIGN IN THE RFP.
 - Poorly written RFPs that have language which cannot be executed
 - Lack of requirement to include Cybersecurity Designers at Charrettes and Design Review meetings from the A-Es and the Government
- WHY IS THIS?
 - The Cyber “Unicorns” are not brought in from the very beginning on “both sides”
 - Cybersecurity for OT is constantly changing due to increased connectivity; makes costs difficult to quantify
 - If Cyber Designer for FRCS is performed correctly, then end client doesn’t “see” this result, (e.g., Leads to mindset of “Cyber isn’t really needed” or “Cyber design costs too much”)

D-B, D-B-B, RMF, RFP, UFC, UFGS.....!



UFC 4-010-06 (2023), Section 1-2, Purpose and Scope: *“This UFC does not implement the RMF and does not address anything beyond the design of the system. Use of this UFC does not result in an ATO under the RMF process but will provide a system that is more capable of receiving an ATO than a system not designed in accordance with this UFC.”*

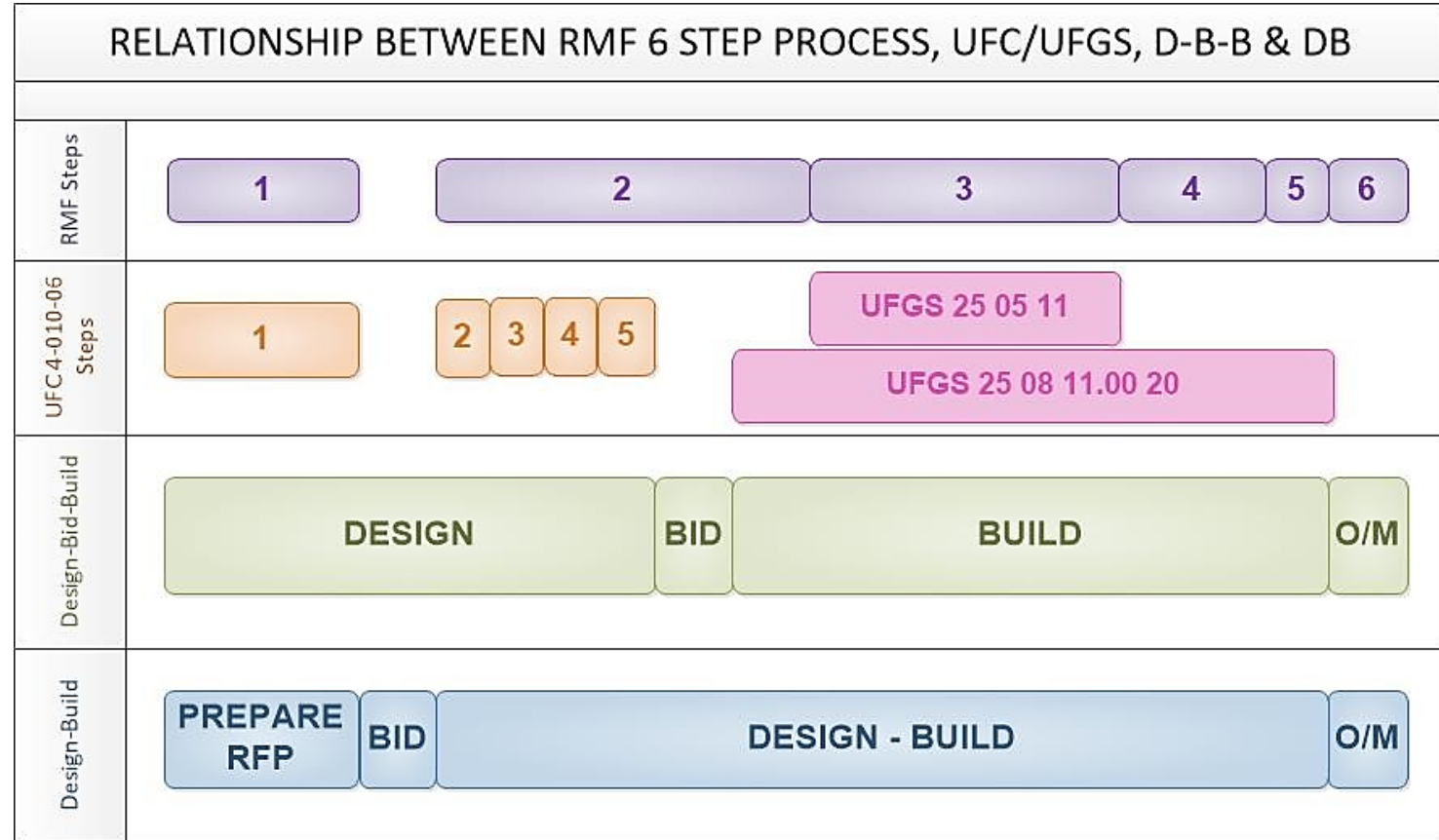
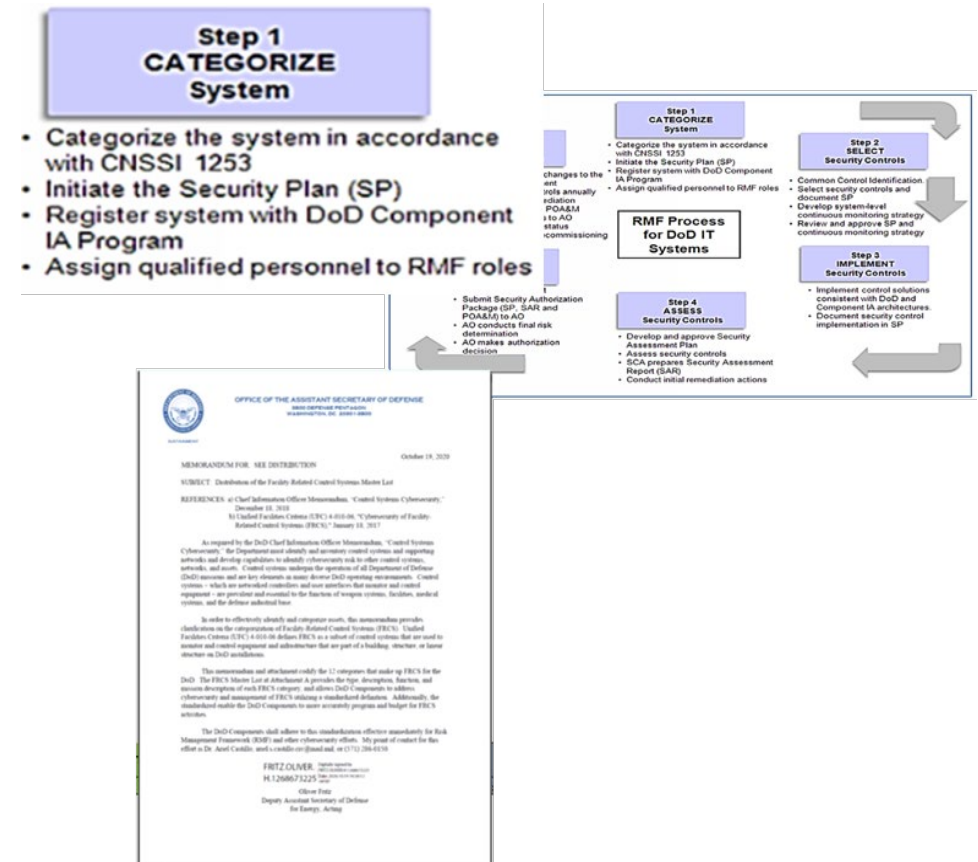


Image used with permission from David A. Gary, Naval Facilities Engineering Command, HQ

Government SHOULD Identify and Categorize Systems BEFORE the RFP Release

- Determine Mission Rating for BLDG/Project (Support, Essential, or Critical)
- Identify all *Potential* Control Systems
- Determine/Verify Control System Impact Loss on the Mission (L/M/H)
- Determine the OT Cybersecurity Government POC (Person or Role) for the Project



A-Es SHOULD Be Educated to Look for Cybersecurity Requirements When Pursuing:

- Is UFC 1-200-01 listed in RFP as a requirements, Yes/No? If Yes, then UFC 4-010-06 is required.
- Do a word search for “Cybersecurity” in the RFP & determine what each reference to the word means.

1.7.7 Phasing of Work, Security, and Construction Staging
 1.7.8 Sustainability
 1.7.8.1 Criteria
 1.7.8.2 Life-Cycle Cost Analysis (LCCA)
 1.7.8.2.1 LCCA Format
 1.7.8.2.2 LCCA Building-Level Analysis
 1.7.8.2.3 LCCA Individual Component or System Alternatives Analysis
 1.7.8.3 Energy Consumption Reduction Requirement
 1.7.8.4 Energy Compliance Analysis (ECA)
 1.7.8.4.1 ECA Narrative Requirements
 1.7.8.5 Total Building Commissioning
 1.7.9 **Cybersecurity**
 1.7.10 Bridging Documents
 1.7.11 Design and Construction Measurement Units
 1.7.12 Personnel Qualifications and Experience
 1.7.13 Design and Construction Deliverables
 1.7.14 Advanced Modeling and Facility Data Requirements
 1.7.15 Operations and Maintenance Requirements
 1.8 OVERVIEW OF DESIGN-BUILD PROCESS
 1.8.1 Overview

SECTION 01 81 00 Page 1

criteria from these sources may be supplemented, but not supplanted, by applicable criteria contained in nationally recognized codes and standards.

	U.S. DEPARTMENT OF DEFENSE (DOD)
DOD 8510.01	(2014; Change 1-2016; Change 2-2017) Risk Management Framework (RMF) for DoD Information Technology (IT)
DODI 8500.01	(2014) Cybersecurity
UFC 1-200-01	(2019) DoD Building Code (General Building Requirements)
UFC 1-200-02	(2016; Change 4, 2019) High Performance and Sustainable Building Requirements
UFC 3-101-01	(2011; Change 5, 2019) Architecture
UFC 3-600-01	(2016; Change 4, 2020) Fire Protection Engineering for Facilities
UFC 4-010-06	(2016; Change 1, 2017) Cybersecurity of Facility-Related Control Systems
UFC 4-021-01	(2008; with Change 1, 2010) Design and O&M: Mass Notification Systems

1.5 DESIGN AND CONSTRUCTION OBJECTIVES

The primary purpose of this project is to create interior spaces tailored to occupying unit operational needs, with a facility functional life of 30 years. See the bridging documents for floor plans, as well as space-by-space requirements for the new facility.

Among the features of work are the following. See individual discipline requirements specifications for additional requirements:

- Design and installation of an air barrier system for the building to meet UFC 3-101-01 and the standards set forth in it.
- Entire work complete for Procurement and Installation of Generator Set and Switchgear, associated controls and monitoring, and connections to fuel system.
- Entire work complete for construction of communications lines and ductbank from the [redacted] facility to Building 1038.
- Entire work complete for **Cybersecurity** documentation and alterations to commercial equipment, services, firmware, and software to satisfy **Cybersecurity** requirements.
- (Bid Option) Procurement and installation of furniture, furnishings, and equipment (FF&E).
- (Bid Option) Procurement and installation of Intrusion Detection System (IDS) and Electronic Security Systems (ESS) to include Facility Access Control System (FACS).
- (Bid Option) Procurement and installation of CCTV system equipment and devices.

SECTION 01 81 00 Page 6

1.7.9 **Cybersecurity**

All control systems (including systems separate from an energy management control system) shall be planned, designed, acquired, executed, and maintained in accordance with DODI 8500.01, DOD 8510.01, NIST SP 800-82, and UFC 4-010-06, and as required by individual Service Implementation Policy. Systems requiring **Cybersecurity** are listed in 01 86 10 MECHANICAL REQUIREMENTS.

- 1.14.3.1 Ceiling Mounted Supply Diffusers
- 1.14.3.2 Ceiling Mounted Return and Transfer Grilles
- 1.15 VENTILATION AND EXHAUST SYSTEMS
- 1.15.1 Exhaust Fans
- 1.15.2 Ceiling Mounted Exhaust Grilles
- 1.16 **CYBERSECURITY**
- 1.16.1 Patch and Update List
- 1.16.2 Documentation Format
- 1.16.3 Miscellaneous **Cybersecurity** Requirements
- 1.17 BUILDING TEMPERATURE CONTROL SYSTEM
- 1.17.1 General DDC Requirements
- 1.17.2 Alarm Monitoring
- 1.17.3 Stand-Alone Operation
- 1.17.4 Input/Output Devices

Live Content Slide

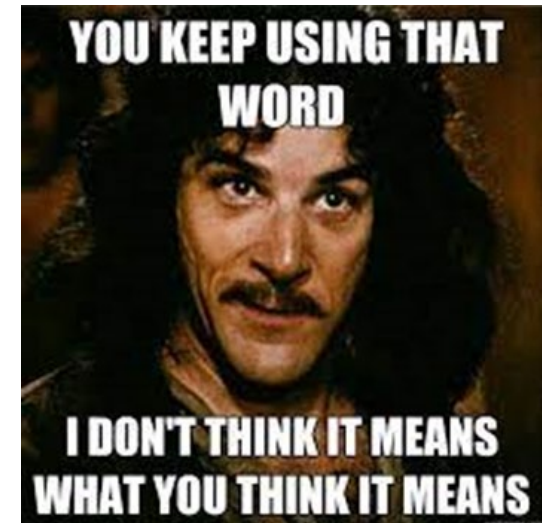
Poll: True or False: Projects that execute UFC 4-010-06 in their contracts, will be able to obtain an Authority to Operate (ATO) with DoD?

RFP Language Examples/Proposed Responses

“Entire work complete for cybersecurity documentation and alterations to commercial equipment, devices, firmware, and software to satisfy cybersecurity requirements.”

Possible, A-E Response:

“The A-E interprets this as ‘Entire work complete for cybersecurity documentation and alterations to commercial equipment, devices, firmware, and software to satisfy cybersecurity requirements’ to mean all documentation as defined in the UFC, where the requirements incorporated into the design are identified according to what is required by the most current UFC 4-010-06 and most current UFGS 25 05 11 at the time of contract execution. Our proposal includes documentation identified in the UFC, and requirements incorporated for systems will be determined based on these requirements but additional RMF documentation (any documentation addressing requirements that can not be addressed as “designer” CCLs as defined in the UFC) is NOT included.”

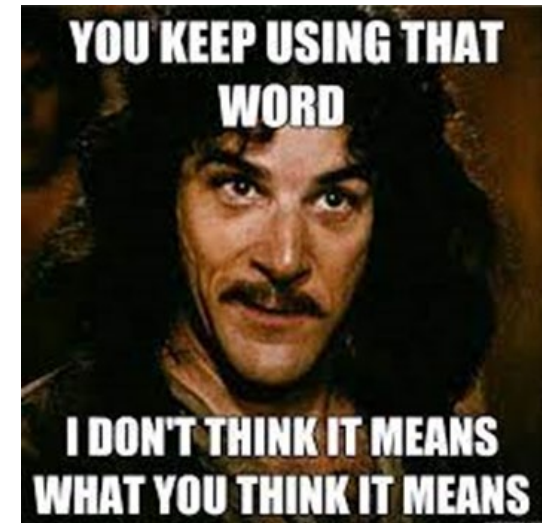


RFP Language Examples/Proposed Responses

“All control systems (including systems separate from an energy management control system) shall be planned, designed, acquired, executed, and maintained in accordance with DODI 8500.01, DOD 8510.01, NIST SP 800-82, and UFC 4-010-06, and as required by individual Service Implementation Policy. Systems requiring cybersecurity are listed in 01 86 10 MECHANICAL REQUIREMENTS.”

Possible, A-E Response:

“The A-E interprets this as ‘All control systems (including systems separate from an energy management control system) shall be planned, designed, acquired, executed, and maintained in accordance with DODI 8500.01, DOD 8510.01, NIST SP 800-82, and UFC 4-010-06, and as required by individual Service Implementation Policy’ to mean all FRCS systems identified shall be planned, designed, acquired, executed and maintained, according to what is outlined and required in Chapter 3 APPLYING CYBERSECURITY IN DESIGN and Section 5-2, Requirements by Design Phase of the most current UFC 4-010-06 at the time of contract execution. Any planning, designing, acquisition, executions and maintenance of Control Systems that can not be addressed as “designer” CCIs as defined in the UFC) is NOT included.”



Designer (SOW) vs Government (RFP) “Language”

A-E “CYBERSECURITY DESIGNER”	GOVERNMENT
Best Estimate of type and number of FRCS Cybersecurity Design Process must be applied to	Best Estimate of type and number of FRCS Cybersecurity Design Process must be applied to
Language states in A-E SOW that assumes these estimated C-I-A Impact Ratings Per FRCS	Estimated C-I-A Impact Ratings Per FRCS are <i>presumed</i> known or <i>presumed</i> to be known by end user
Language states in A-E SOW that assumes the Authorizing Official	Authorizing Official is <i>presumed</i> known or <i>presumed</i> to be known by end user
Language states in A-E SOW that assumes the POC for the ISSM and/or ISSO (e.g., NAVFAC CIO 2/4; TACOM G6 CIO)	The POC for the ISSM and/or ISSO (e.g., NAVFAC CIO 2/4; TACOM G6 CIO) is <i>presumed known</i> or <i>presumed</i> to be known by the end user
Language states in A-E SOW that assumes the Cybersecurity SME(s) will be onsite for the Kickoff meeting, Charrette & at least virtually for all other DRCs	May or may not require a Cybersecurity SME for the project onsite or virtually depending on the project, knowledge of the RFP government author etc.
Language states in A-E SOW that assumes there will be a separate Cybersecurity Design Review between 35-65% DRC.	Usually, no requirements for any Cybersecurity at Charrette and Design Reviews (DRs); Cybersecurity may, if included, get 30 minutes tops and may not have a Government personnel needed

Designer (SOW) vs Government (RFP) “Language”

A-E “CYBERSECURITY DESIGNER”	Possible, A-E Example Language to use in SOW:
Best Estimate of type and number of FRCS Cybersecurity Design Process must be applied to	The A-E will use as its baseline for identification of all control systems the 12 categories that make up FRCS for the DoD based on The Office of the Assistant Secretary of Defense, MEMORANDUM FOR: SEE DISTRIBUTION, SUBJECT: Distribution of the Facility-Related Control Systems Master List, and its attachment, Addendum -FRCS Master List.
Language states in A-E SOW that assumes these estimated C-I-A Impact Ratings Per FRCS	The A-E will assume that the Authorizing Official shall be the NAVY as defined by DoD as the real-property owner.
Language states in A-E SOW that assumes the Authorizing Official	The A-E will assume that the Point of Contact for all Cybersecurity Design Process Applications shall be NAVFAC CIO 2 (insert region here).
Language states in A-E SOW that assumes the POC for the ISSM and/or ISSO (e.g., NAVFAC CIO 2/4; TACOM G6 CIO)	This meeting will verify the project scope and expectations, highlight coordination issues, etc. with the client and government representatives. This meeting will last two hours (not including preparation and follow-up effort) and must be attended by the key members of the AE’s Design Team who will be working on this T.O. to include: AE’s Project Manager, Architect, Structural Engineer, Mechanical Engineer, Electrical Engineer, Civil Engineer, Landscape Architect, Cost Engineer, Fire Protection Engineer, Interior Designer, CTS-D, Cybersecurity Control Engineers, and Geotechnical Engineer.
Language states in A-E SOW that assumes there will be a separate Cybersecurity Design Review between 35-65% DRC.	This meeting will be in accordance with FC 1-300-09N and will be an initial concept meeting to discuss the requirements and technical features required for the control systems which will be applicable to the project. The intent of this meeting will be to confirm Security Controls & CCI Final Acceptance of all Control Systems all control systems identified according to the Mission C-I-A ratings received from Installation Systems Security Manager in the FRCS Review Meeting II and confirm the RMF Categorization Submission applicable to all FRCS identified prior to the 65% “over the should” Design Review Meeting.

Practical Summary of Potential Costs to PCRs, PDRs, PCAS, DBs, and DBBs



2024

JOINT ENGINEER
TRAINING CONFERENCE
& EXPO

SAMEJETC.ORG



[@PSAMENATIONAL](https://www.facebook.com/PSAMENATIONAL)



[@PSAME_NATIONAL](https://twitter.com/PSAME_NATIONAL) | [#SAMEJETC24](https://twitter.com/SAMEJETC24)

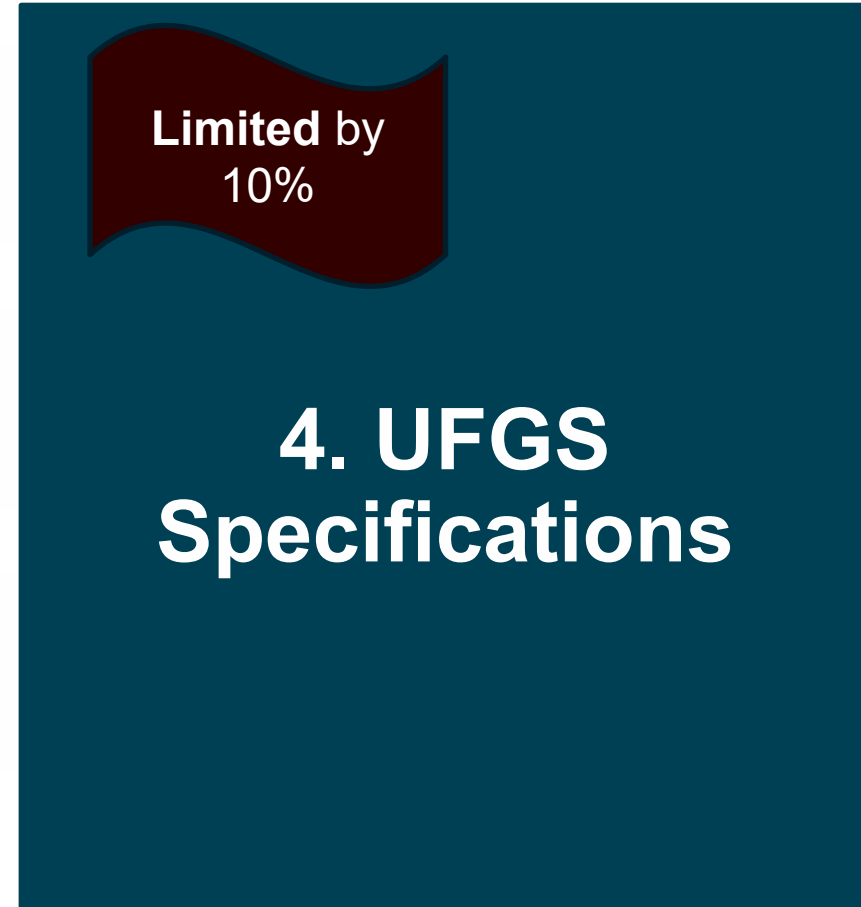
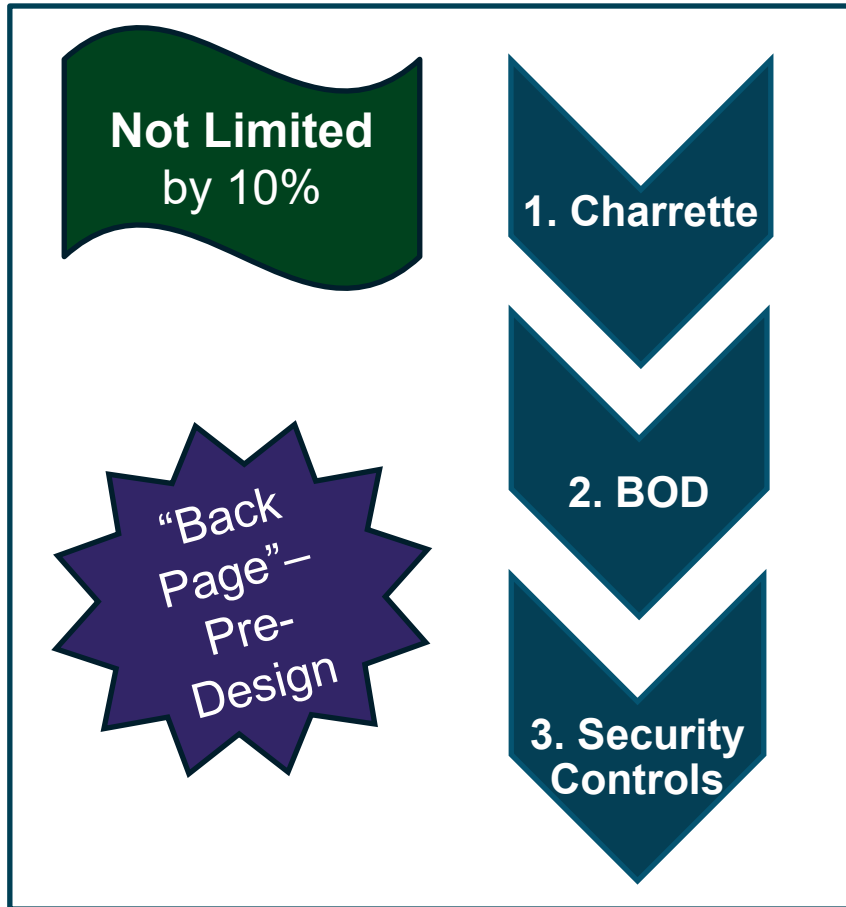


["SOCIETY OF AMERICAN MILITARY ENGINEERS"](https://www.linkedin.com/company/society-of-american-military-engineers)

Live Content Slide

Poll: True or False: Once Control Systems and their ratings are identified, there shouldn't be any Design "Scope Creep" for Cybersecurity allocated budgets.

Federal/DoD Design Fee – 10% Fee Limitation



SCOPE/BUDGET Causes for Variance in Design

- **Direct Impact:**
 - Mission Rating (Support / Essential / Critical)
 - Number of Asset Groups (HVAC, FLS, etc.)
 - Asset C-I-A and Mission Ratings (L, M, H)
 - Connectivity or Provision of a Front-End System
- **Indirect Impacts:**
 - Charrette Attendance by Client ISSM/ISO
 - Charrette Attendance by AE Cybersecurity Designer, SME
 - Lack of coordination efforts between Engineers, Cybersecurity Designer, and Client's Control System Owner/Operator
 - RFI Response Timeliness / Accuracy from Client



Image from CIMON

BUILD/IMPLEMENTATION Cost Impacts

Direct Impacts:

- Per 25 05 11.XX Section
 - Up to 27 Submittals
 - Cyber Support, Testing & Training Hours
- 25 10 10
 - Up to 6 Submittals
 - Up to 3 PVTs
- 25 08 10
 - Up to 6 Submittals
 - Off-Site Factory Tests
 - Documented Test Plans
 - 2 PVTs
- 25 08 11.00 20 (NAVY)
 - 10 Submittals
 - 5 Cybersecurity Tests
 - eMASS Access
 - Additional Qualifications for ATO

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.

Submit [four][_____] copies of the Control System Cybersecurity Testing Report. The Control System Cybersecurity Testing Report may be submitted as a Technical Data Package.

3.15 FIELD QUALITY CONTROL, CYBERSECURITY VALIDATION SUPPORT

In addition to testing and testing support required by other Sections, provide a minimum of [_____] 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.

3.14.1 Control System Cybersecurity Testing Procedures

Prepare 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.

Submit [4] [_____] copies of the Control System Cybersecurity Testing Procedures. 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 TESTING 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 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

CYBERSECURITY TRAINING

Provide [eight][_____] hours of classroom [and hands-on] training for [_____] Government personnel on the cybersecurity operation and maintenance of the control system provided. This training is in addition 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 --

Contractor Required Submittals

25 05 11.XX Contractor Submittals Per FRCS System

- SD-01 Preconstruction Submittals
 - Wireless & Wired Communications Broadcast Requests
 - Device Account Lock Exception Requests
 - Multiple IP Connection Device Requests
 - Contractors' Computer Cyber Compliance
 - Temp Contractors' Computer Cyber Compliance
 - Cybersecurity Interconnection Schedule
 - **Protection of Information at Rest Protocol**
 - **Proposed STIG/SRG Applicability Report**
 - Qualifications
- SD-02 Shop Drawings
 - Network Communications Report
 - Cyber Riser Diagram
- SD-06 Test Reports
 - Wireless Communications Test Reports
 - **Control System Cybersecurity Testing Procedures**
 - **Control System Cybersecurity Testing Reports**
- SD-07 Certificates
 - Software Licenses
- SD-11 Shop Drawings
 - **Password Change Summary Report**
 - Enclosure Keys
 - Software **and Configuration** Backups
 - **Auditing Front End Software**
 - **Device Audit Record Upload Software**
 - **System Maintenance Tool Software**
 - **Control System Scanning Tools**
 - **STIG, SRG & Vendor Guide Compliance Result Report**
 - Control System Inventory Report
 - **Integrity Verification Software**

Contractor Required Submittals

25 08 10 Contractor Submittals for 25 05 11.XX if Computer Front-End Provided

- SD-06 Test Reports
 - PVT Plan
 - PVT Phase I Report
 - PVT Phase II Report
- SD-07 Design Data
 - Test Instrumentation Calibration Report
 - Cyber Riser Diagram

25 10 10 Contractor Submittals for 25 05 11.XX if Computer Front-End Provided

- SD-02 Shop Drawings
 - UMCS Contractor Design
 - Drawings
 - Draft As-Built Drawings
 - Final As-Built Drawings
- SD-03 Product Data
 - Product Data Sheets
 - Computer Software
 - Enclosure Keys
- SD-05 Design Data
 - UMCS IP Network Bandwidth Usage Estimates

- SD-06 Shop Drawings
 - Pre-Construction QC Checklist
 - Existing Conditions Report
 - Post-Construction QC Checklist
 - Factory Test Procedures
 - Factory Test Report
 - Start-up & Start-up Testing Report
 - PVT Phase I Procedures
 - PVT Phase I Report
 - PVT Phase II Report
- SD-10 Operation and Maintenance Data
 - Operations & Maintenance Instructions
 - Preventative Maintenance Workplan
 - Basic, Advance & Refresher Training Documentation
- SD-11 Closeout Submittals
 - Closeout QC Checklist
- Testing Requirements
 - Factory Acceptance Testing
 - Phase I Testing
 - Phase II Testing

Contractor Required Submittals (NAVY Only)

25 08 11.00 20 Contractor Submittals that Coincide with 25 05 11.XX

- SD-01 Preconstruction Submittals
 - Authorization Strategy Plan
- SD-05 Design Data
 - CCI List
 - Security Plan
 - Ports, Protocols and Services Management Registration Form
- SD-06 Test Reports
 - ACAS Vulnerability Reports
 - STIG Checklists
 - SCAP Scan Reports
 - ISSE Checklist Step 3
 - ISSE Checklist Step 4
- SD-03 Product Data
 - Product Data Sheets
 - Computer Software
 - Enclosure Keys
- SD-07 Certifications
 - IAM/IAT Level II Certification Qualification
- Per System Non-Submittal Activities
 - Execute SCAP Scans (where applicable)
 - Execute ACAS Vulnerability Scans (where applicable)
 - Execute STIG Checklists
 - Provide POA&M Documentation
 - Assist with SCA-V Site Assessment
 - RMF Step 2 Check Point Meeting
 - RMF Step 3 – Submittal Uploads (5 Submittals)
- Per System Non-Submittal Activity
 - CAC Registration
 - Construction Coordination Meeting



DD1391 Programming Guide

DD1391 PROGRAMMING GUIDE

NAVY/Marines (NAVFAC Projects)

Primary Facilities

- \$100k for projects under \$10M
- 1% for projects over \$10-50M
- \$500k for projects over \$50M

Non-Facility Projects

- \$50k for ECC under \$10M
- 0.5% for \$10M < ECC under \$50M
- \$250k for project over \$50M

Cybersecurity Commissioning (All projects)

- 0.5% of PRIM FACS + ELEC/MECH Costs
 - 0.25% to contractor (50%)
 - 0.25% to CIO costs (50%)

AIR FORCE/ANG

Commissioning

- \$100,000 for projects under \$10M
- 1% for projects \$10M < ECC under \$50M
- \$500,000 for projects over \$50M

Special Cyber Features

- \$100,000 for projects under \$5M
- \$250,000 for projects over \$5M

ARMY (USACE)

\$250k per platform

Deep Dive Analysis of Chapter 5 Section 5-4 “REQUIREMENTS BY DESIGN PHASE”



2024

JOINT ENGINEER
TRAINING CONFERENCE
& EXPO

SAMEJETC.ORG



[@PSAMENATIONAL](https://www.facebook.com/PSAMENATIONAL)



[@PSAME_NATIONAL](https://twitter.com/PSAME_NATIONAL) | [#SAMEJETC24](https://twitter.com/SAMEJETC24)

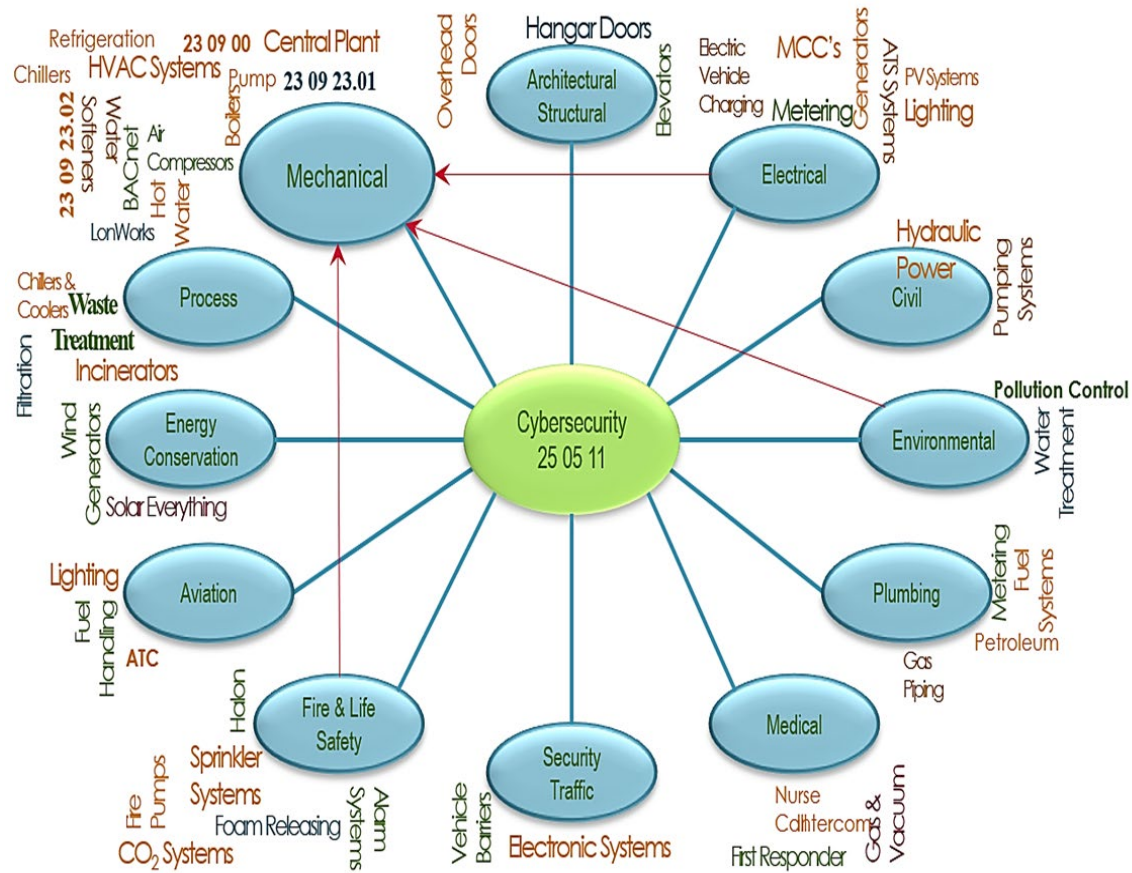


["SOCIETY OF AMERICAN MILITARY ENGINEERS"](https://www.linkedin.com/company/society-of-american-military-engineers)

Live Content Slide

Poll: True or False: Cybersecurity Design SMEs ONLY need to be pulled in AFTER the 35% Design Issuance.

Cybersecurity Design Is a Team Sport



- Interdisciplinary Partners/PEs Leads MUST be Engaged EARLY on BOTH sides
- Early Engagement Controls Risks
 - Engagement During RFP, TO, & Pursuit
 - Engagement During Charrette and DRCs
- Cybersecurity is Required **REGARDLESS** of Network Connectivity
 - DoD systems (e.g., weapons systems, stand-alone systems, control systems, or any other type of systems with digital capabilities) must receive and maintain a valid authorization before beginning operations.

What's The Difference Between the "Old" & "New"?

UFC 4-010-06
10 October 2023

CHAPTER 5 CYBERSECURITY DOCUMENTATION

This chapter describes cybersecurity documentation that is required as part of the control system design package. This documentation is in addition to the documentation required by the relevant control system design criteria.

5-1 OVERVIEW.

Cybersecurity documentation for control system design documents the security controls and CCI's applied to the control system along with assumptions made regarding CCI selection, implementation, and information required by others.

5-2 USE OF GUIDE SPECIFICATION.

The design specifications for control system cybersecurity developed in accordance with this UFC must derive from UFGS 25 05 11.

For projects designed by or for USACE, develop separate cybersecurity specifications for each system type and for each impact level. This prevents misinterpretation of specification requirements. Use fourth level numbering of the specification to differentiate the specification by system. Different fourth level numbering schemes are possible; the scheme that is clearest for the project should be used and should be used across the entire project. Two example schemes are using sequential numbering (such as Section 25 05 11.01: Low Impact HVAC, Section 25 05 11.02: Low Impact Lighting Controls, Section 25 05 11.03: Moderate Impact HVAC Controls, etc.) or using numbering that aligns with the division that the control specification is in (such as Section 25 01 11.23: HVAC, Section 25 05 11.26: Lighting). Note that the second scheme becomes unusable when multiple different systems have the same division number, or there are multiple systems of the same type but with different impact levels.

5-3 COORDINATION WITH OTHER DISCIPLINES

As discussed in CHAPTER 3, in order to develop a specification properly aligned with site choices, several design steps must be coordinated with other disciplines. To facilitate this coordination, an optional reference Cybersecurity Design Coordination Worksheet is posted on the Whole Building Design Guide document page for this UFC (<https://www.wbdg.org/ffc/dod/unified-facilities-criteria-ufc-4-010-06>).

5-3.1 Determination of Points of Contact

For this document, the primary points of contact are the System Owner (SO) and the Authorizing Official (AO) for the determination of the C-I-A Impact ratings. In addition there may be coordination with the controls designer, if this individual is separate from the cybersecurity designer, and possibly the SO and AO for the discussion of cybersecurity controls that are not feasible for the FRCS.

39

Notice page numbers:
39 verses 19 =
20+ more pages

Notice New UFC Lists
New Section
"COORDINATION WITH
OTHER DISCIPLINES"

Notice Old UFC lists one
task for 10-15%

Notice NEW UFC does
not even start to list what
is due for the
Design Issuance yet

UFC 4-010-06
19 September 2016
Change 1, 18 January 2017

CHAPTER 5 CYBERSECURITY DOCUMENTATION

This chapter describes cybersecurity documentation that is required as part of the control system design package. This documentation is in addition to the documentation required by the relevant control system design criteria.

5-1 OVERVIEW.

Cybersecurity documentation for control system design documents the security controls and CCI's applied to the control system along with assumptions made regarding CCI implementation and information required by others.

5-2 REQUIREMENTS BY DESIGN PHASE.

Cybersecurity documentation requirements are indicated here by typical Design-Build or Design-Bid-Build design submittals. If the design is using a different submittal schedule, adjust accordingly.

The requirements here reference the five step cybersecurity design process defined in CHAPTER 3.

5-2.1 Basis of Design.

Provide a single submittal indicating the C-I-A impact level for the control system and listing the security controls generated during Step 2 along with recommendations and justifications for further tailoring of the security control set.

5-2.2 Design Submittals.

5-2.2.1 Concept Design Submittal (10-15%).

Provide a single submittal indicating the CCIs resulting from the approved tailored security control list (Step 3) and an initial classification for each CCI (Step 4).

5-2.2.2 Design Development Submittal (35-50%).

Provide a single submittal documenting the following:

- The final classification of each CCI (Step 4).
- The changes to standard CCI requirements identified in Step 5, along with an explanation of the changes.
- The CCIs which have been incorporated into the control system design (Step 5). Document changes from standard requirements, or selections made when multiple options are available. Otherwise, it is not necessary to document the details of the requirement, just whether a specific CCI has been incorporated.
- Information for others as required (Step 5)

19

What's The Difference Between the "Old" & "New"?

UFC 4-010-06
10 October 2023

5-3.2 UFGS Coordination Issues

- For UFGS 25 05 11, there are many designer options that require input from the control's designer, SO, AO, and site personnel. Major consideration includes the following:
 - Whether wireless will be allowed. If so, where? How will it be secured? How will it be tested?
 - User Interfaces. Where will they be located? Which, if any, will be privileged? How will they be secured?
 - User Interface behavior such as session termination and unsuccessful login handling
 - Specific requirements for Fire Protection systems
 - Submittal review. Specific details about documentation, level of inventory reporting, and other submittal requirements
 - Specific hardware or software requirements: Ethernet switches, web and database servers, and device and equipment power.
 - Auditing: front-ends, software, storage capacity, and information system monitoring
 - User Authentication: PKI, passwords, and setting of passwords
 - Cybersecurity testing and training: Field QC, PVT, level of training

5-4 REQUIREMENTS BY DESIGN PHASE.

Cybersecurity documentation requirements are indicated here by typical Design-Build or Design-Bid-Build design submittals. Some of these will require new design documents while others add requirements to design documents that are already required by other criteria or project requirements. The percentage design levels provided here are notional only to demonstrate the order and extent of information needed by each submittal. If the design is using a different submittal schedule, adjust accordingly. The documentation requirements here apply per system and impact level – if the project includes multiple systems or impact levels, a copy of the required documentation for each is required. Submittal templates are posted to the document page for this UFC.

The requirements here reference the five-step cybersecurity design process defined in CHAPTER 3.

40

Notice Old UFC has already finished listing tasks due at each design phase

Notice New UFC Lists New Section "UFGS Coordination Issues"

Notice NEW UFC **STILL** has not listed what is due for the Design Issuance Yet

UFC 4-010-06
19 September 2016
Change 1, 18 January 2017

The recommended format for this submittal is to use the format of \10/1/ with the addition of a column to document the required information.

5-2.2.3 Pre-Final Design Submittal (90%).

Provide a submittal updating the Design Development Submittal with complete final information.

5-2.2.4 Final Design Submittal (100%).

Provide a submittal updating the Pre-Final Design Submittal with complete final information.

20

CANCELED

What's The Difference Between the "Old" & "New"?

UFC 4-010-06
10 October 2023

5-4.1 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).

5-4.2 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).

5-4.3 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:

41

UFC 4-010-06
10 October 2023

- ◊ 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.

5-4.4 Final Design (Unreviewed 100%).

At the Final Design (Unreviewed 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.

5-4.5 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 (Unreviewed 100%) with updated Issued for Construction information.

42

Notice New UFC list SPECIFIC Requirements Starting at 10-15%

Notice New UFC Lists SPECIFIC requirements at 50-65%

Notice NEW UFC Requires One Line Riser Diagrams

Notice NEW UFC Requires Control Systems Connection Descriptions

Notice NEW UFC is almost COMPLETED for Cybersecurity Design by 65% verses OTHER Disciplines are "ramping up"

What's The Difference Between the “Old” & “New”?

“Normal” Cybersecurity Design Coordination Questions

- Who is the POC Cybersecurity Reviewer for FRCS Cybersecurity for all Design Issuances for Project up through the Ready-To-Advertise? (name, position, email)
- Who is the Cybersecurity Point of Contact (POC) responsible for Facility-Related Control Systems (FRCS) on the installation/base? (name, position, email)
- Who is the Authorizing Official (AO) and their contact information (name, position, email)?
- What is the facility classification (Mission Support, Mission Essential, Mission Critical) for Building 3089?
- Who is the person who is directly responsible for each control system identified (name, position, email)? Is this person the same as the System Owner (SO) for each control system? (If no, provide name, position, email for each system if it is a different person)
- Who is the technical person for cybersecurity questions the Cybersecurity Designer and the Contractor can go to for questions who is directly responsible for the FRCS? (name, position, email)
- Who is the person who will have responsibility for day-to-day operations and maintenance of the FRCS and the controlled equipment? (name, position, email for each control system identified)?
- Is there an Authority To Operate (ATO) for any of the identified FRCS? If yes, what is their C-I-A Loss of system impact rating(s)?
- Do any of the Control Systems identified have a Justification and Authorization (J&A) for them?

What's The Difference Between the “Old” & “New”?

“New Contractor” Cybersecurity Design Coordination Questions To Answer

- Are read-only actions allowed from a UI (that supports accounts) if a user is not logged in for any system according to site policy?
- Are there any User Interfaces which require protection because of Confidentiality concerns in the system according to site policy?
- Would the site prefer a report providing the device passwords, or would the site prefer to have a person accompany the contractor and change the passwords themselves?
- For controllers and computers, how many audit records should those devices be able to store locally at the device according to site policy?
- Will software for the identified FRCS need to be purchased? If yes, How long should the software be licensed for? Who should the software be licensed to (the project site or the government)?
- Contractors are required to review STIGS for applicability but may not have access to them. Who will be the POC to provide/justify access? (name, position, email)
- Confirm that wireless is not authorized for this project. (Or can Contractor's use temporary Wireless Network?)
- There may be some devices a Contractor would purchase that cannot meet stated password requirements. The default is to reject those devices; yes, or no?
- How many hours should the contractor should allot for validation testing for the LOW Systems before and after Cybersecurity requirements have been applied to ensure control systems are fully functional as designed after Cybersecurity has been applied?
- How many hours should the contractor should allot for their participation in RMF validation testing for the LOW Systems in addition to and separate from the Cybersecurity Testing which is required?
- Will the Client require that the Contractor have a Control System Cybersecurity Subject Matter Expert to oversee the execution of all 25 05 11 specifications throughout the duration of the construction who is qualified according to DODI 8140? If yes, choose the qualifications: IAM L1; IAM L2; IAT 1; IAT 2; IAM and IAT L1; IAM and IAT L2
- Will the Client allow for a single person who meets the DoDI 8140 requirements to serve across the entire contract? Yes/No?

What's The Difference Between the “Old” & “New”?

“New MODERATE” Cybersecurity Design Coordination Questions To Answer

- Several Cybersecurity requirements vary depending on whether the item is inside "mission space". Who will be the POC for Physical Security to determine boundaries of mission space and indicate on contract requirements to ensure requirements for the MODERATE rated Control System?
- Many MODERATE Cybersecurity requirements related to User Interfaces (UIs) depend on whether the UI is "privileged", Who will be the POC to coordinate with to determine which UIs are privileged for the MODERATE rated Control System?
- Use of "standard" database servers and web servers on computers can facilitate cybersecurity since the site is generally more familiar with standard software packages. Are there any software packages are allowed by the site for the MODERATE Control System? Are there any software packages which are NOT allowed by the site for the MODERATE control System?
- To what extent should User Interfaces lock the interface after unsuccessful login attempts, for how long, and how should the lock-out be released for the MODERATE System? Are there specific interfaces that, because of high availability requirements, should not be locked in the MODERATE System?
- How soon should session lock be initiated after cessation of activity, for session termination and are there exceptions to this for the MODERATE system?
- Are there any requirement for multi-factor authentication (typically PIV or CAC) or are there user interfaces with specific requirements? Especially for the MODERATE System. If yes, does the site want the contractor to help set up PKI infrastructure in the system?
- For the MODERATE System, does the site have existing software? What is it? Who will be the POC to help contractor determine if it is compatible with the provided control system to meet all the required auditing requirements?
- How should the MODERATE control system respond to auditing processing failures?
- How many copies of the Cybersecurity testing procedures and test report should the contractor provide?
- For the MODERATE System, does the system need malware protection software licenses, software media, neither, or both?
- Are there any additional requirements for system monitoring for the MODERATE System?

What's The Difference Between the "Old" & "New"?


"LEST YE DOUBT...."

wbdg.org/fc/dod/unified-facilities-criteria-ufc-4-010-06

ESTCP Contr... DoD Publications TOR Scanning Gmail Unified Facilities Cri... Hacking Interests DoD Directives and... DAU Marketing Research Army Publishing Dir... Conferences Reque... Anime

DESIGN RECOMMENDATIONS PROJECT MANAGEMENT TOOLS FEDERAL FACILITY CRITERIA CONTINUING EDUCATION ADDITIONAL RESOURCES

DEPARTMENT OF DEFENSE / UNIFIED FACILITIES CRITERIA (UFC) / UFC 4-010-06 CYBERSECURITY OF FACILITY-RELATED CONTROL SYSTEMS (FRCS)



UFC 4-010-06 Cybersecurity Of Facility-Related Control Systems (FRCS)

Date: 10-10-2023
Series: 4 - MULTI-DISCIPLINARY AND FACILITY-SPECIFIC DESIGN
Status: Active

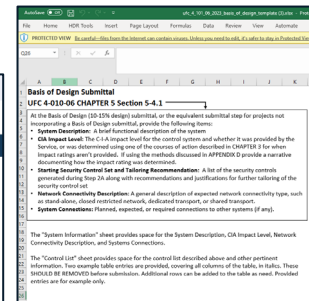
This UFC describes requirements for incorporating cybersecurity in the design of all facility-related control systems which include a network. This UFC covers the cybersecurity aspects of control system design, and the requirements of this UFC must be coordinated with the control system design and the criteria relevant to the control system. This UFC only covers aspects specific to control system design. Many projects have IT-specific components (such as IP network design security) which are not covered by this UFC; in those cases, the controls designer will need to coordinate with other disciplines. This UFC defines a process for identification of cybersecurity requirements based on the Risk Management Framework suitable for control systems of any impact rating and provides specific guidance suitable for control systems assigned LOW or MODERATE impact level.

This UFC covers the incorporation of cybersecurity concepts and requirements in support of the Risk Management Framework. This UFC does not supplant the RMF and does not address anything beyond the design of the system. Use of this UFC does not result in an ATO under the RMF process but will provide a system that is more capable of receiving an ATO than a system not designed in accordance with this UFC.

Page(s): 258
View/Download: PDF

Related Materials: Cybersecurity Design Checklists (10-13-2023)
Cybersecurity UFGS Parser (10-13-2023)
Basis of Design Submittal Template (10-10-2023)
Concept Design Submittal Template (10-10-2023)
Interim Design Submittal Template (10-10-2023)
CGI Generator - Simplified (10-10-2023)
Control and CCI List Maker (10-10-2023)
UFC Appendix G - CCI Tables (10-10-2023)

Criteria Change Request: CR

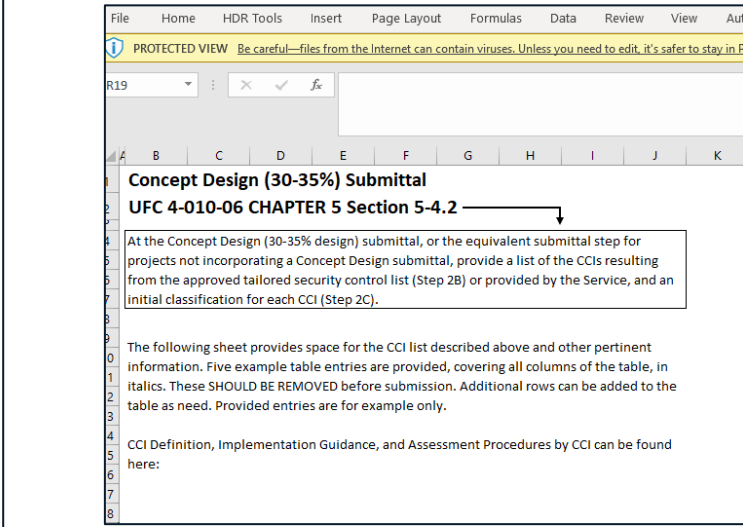


Basis of Design (10-15%) Submittal

System Name: _____
System Description: _____
C-I-A Impact Level: Confidentiality Integrity Availability
Source: Determined by UFC 4-010-06 Chapter 3
Additional Narrative: _____
(Required when not Provided)

Network Connectivity Description: Stand Alone/Closed/Restricted
Additional Narrative: _____
(Not Required)

System Connections: _____
(If Any)



Concept Design (30-35%) Submittal
UFC 4-010-06 CHAPTER 5 Section 5-4.2

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).

The following sheet provides space for the CCI list described above and other pertinent information. Five example table entries are provided, covering all columns of the table, in italics. These SHOULD BE REMOVED before submission. Additional rows can be added to the table as needed. Provided entries are for example only.

CCI Definition, Implementation Guidance, and Assessment Procedures by CCI can be found here:

Starting Control Set and Tailoring Recommendations

Control Number	Control Title	Control List	Status (Add, Remove, or Generate)	Comments
AC-2	Access Control Policy And Procedures	Description: The organization: (a) develops, documents, and disseminates to (Assignment/ Implementation/Defeat/Prevention or other);		generated by designer
AC-2(1)	User-Managed Digital Objects / Message Delivery	Description: The information system: (a) provides a digital signature for user-managed communications sessions whenever authentication is used for guest access to;	Remove	Assessment based on CCI table display

Interim Design Submittal
UFC 4-010-06 CHAPTER 5 Section 5-4.3

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.

The "System Connections" sheet provides a table for the System Connections information. The first line in italics provides an example of a table entry. This SHOULD BE REMOVED before submission. Additional rows can be added to the table as needed. Provided entries are for example only.

The "CCI List" sheet provides space for the CCI list described above and other pertinent information. Five example table entries are provided, covering all columns of the table, in italics. These SHOULD BE REMOVED before submission. Additional rows can be added to the table as needed. Provided entries are for example only.

Redline Specifications and Drawings and Riser Diagrams should be attached separately.

CCI Definition, Implementation Guidance, and Assessment Procedures by CCI can be found here:

***The Final Design (Unreviewed 100%) Submittal is the Finalized version of the submitted Interim

What's The Difference Between the “Old” & “New”?

- ***A-Es MUST Begin Planning AND Asking for Early Engagement From The Government To Accomplish All of Chapter 5 Requirements!***
- THE PROJECT DESIGN CHARRETTE Estimated Duration of Discussion is 2 HOURS for FRCS Cyber ONLY
- Project Management Team and Designer of Record Cybersecurity SME to PLAN, PLAN, PLAN BEFORE the Design Charrette to ensure all stakeholders are present
- If this information is NOT gained during the charrette, the project may experience delays or worst yet, incomplete cybersecurity design exposing our nation's warfighters to threats via Facility-Related Control Systems
- ***Sample Charrette Agenda Provided by: Susan Howard, National ICS/OT Cybersecurity Lead at Michael Baker International***

1. Validate which control systems will be included – requires all engineering stakeholders present:
 1. Fire Systems – will they be IP based?
 2. HVAC Building Control Systems – will these be connected to an existing basewide Front End?
 3. Electrical systems – Lighting, Generators, Substations, Microgrid systems, others?
 4. Cranes – YES – Cranes require cybersecurity especially on NAVFAC projects www.whitehouse.gov/administration-announces-initiative-to-bolster-cybersecurity-of-u-s-ports/
 5. Water treatment systems
 6. Elevators
 7. ESS – will Security Forces be engaged
2. Designer of Record Cyber to gather names and contact information for all stakeholders
3. Who will be the System owner for each? DPW, PWD, Fire Chief, Security Forces?
4. Confirm if the Authorizing Official will be NAVFAC, AFCEC, OR USACE
5. What are recommended C-I-A System Impact Levels for EACH control system?
6. Are there existing Authority To Operate (ATOs) for any of these control systems?
7. Any J&A's (Justification and Authorization i.e. Sole Source) in existence for any control system?
8. What are interconnections for each control system?
9. What are data protocols? Authorization Boundaries? Transport Data Flow information?
10. How Many UFGS 25 05 11 specs estimated?
11. What will the authorization strategy be for each control system?

What's The Difference Between the "Old" & "New"?

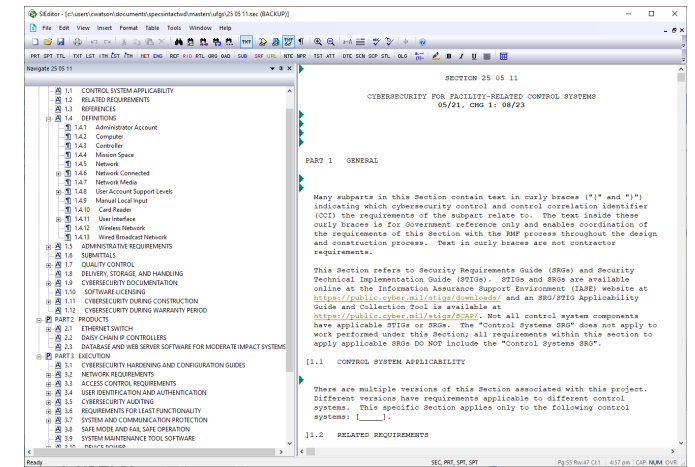
NOW, UFGS and CCI Design Tailoring and Editing Can Begin

AutoSave [m] ufc_4_101_06_2023_interim_design_template (9).xlsx - Protected View • Saved to this PC

File Home HDR Tools Insert Page Layout Formulas Data Review View Automate Help BLUEBEAM Power Pivot

PROTECTED VIEW Be careful—files from the Internet can contain viruses. Unless you need to edit, it's safer to stay in Protected View. Enable Editing

Control Number	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Enclave	Designer	Non-Designer	Impractical	DoD Defined	Not Applicable to RCS	Justification for N/A to RCS UFC Table H-2	Removed from Low Baseline	Rationale for removal from Low Baseline UFC Table H-3	UFGS 230511 Reference	Implementation Status
AC-1	000001	The organiza	The organization bein	The organization conducting		X									
AC-8	001384	The informat	The organization bein	The organization conducting					X	CS is not publically acce				Not Applicable to FRCS; Control Systems are not publically access	
CP-2	000443	The organiza	The organization bein	The organization conducting		X								Applicable only to Control Systems with essential mission functi	
CP-7(1)	000516	The organiza	The organization bein	The organization conducting	X		X								
CP-8	000522	The organiza	DoD has defined the	The organization being inspe	X			X							



Review of the new Appendix D: Considerations in Determination of Control System Impact Ratings and what this means for the C-I-A Impact Ratings



2024

JOINT ENGINEER
TRAINING CONFERENCE
& EXPO

SAMEJETC.ORG



[@PSAMENATIONAL](https://www.facebook.com/PSAMENATIONAL)



[@PSAME_NATIONAL](https://twitter.com/PSAME_NATIONAL) | [#SAMEJETC24](https://twitter.com/SAMEJETC24)



["SOCIETY OF AMERICAN MILITARY ENGINEERS"](https://www.linkedin.com/company/society-of-american-military-engineers)

Live Content Slide

Poll: What is the FIRST Step in Designing Cybersecurity For a Control System?

Five Steps for Cybersecurity Design Process

3-2 STEP 1: DETERMINE CONTROL SYSTEM IMPACT RATING.

The SO, with concurrence from the AO, determines the impact levels of the control system. The SO may seek assistance from the control system designer in defining the functionality of the control system, the information the control system contains, and the impact of failure of the control system. For the DoD, impact levels are determined based on the mission of the relevant Service and in many cases can use the mission criticality rating of the facility (mission support, mission essential, mission critical) as a starting point to determining control system impact. It's also important to note that while a traditional information system generally prioritizes Confidentiality, then Integrity and lastly Availability, control systems usually prioritize Availability first, then Integrity and lastly Confidentiality.

If impact ratings aren't provided, request them from the Service. If the Service is unable to provide impact ratings then request direction from the Service and follow one of two courses of action as directed:

1. Use the "starting" impact ratings for the control system type and facility rating (mission support, mission essential, mission critical) from the Control System Master List available at the RMF Knowledge Service website (<https://rmfks.osd.mil>).
2. Do not proceed with the design until C-I-A Impact ratings are provided.

3-1.1 Five Steps for Cybersecurity Design.

The five steps for cybersecurity design are:

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: Using the DoD master Control Correlation Identifier (CCI) list, create a list of relevant CCIs based on the controls selected in Step 2A.

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.

For both "Old" and "New" version Step 1 is to determine the Control System's Impact Rating. This has not changed.

New Directions to “ASSUME” C-I-A

- There are now ways to “assume” C-I-A Loss of System Impact Ratings
- Goal is to allow the Cyber Designer to:
 - Move forward with choices of overlays
 - Move forward with choices of Control Correlation Identifiers tailoring
 - Move forward with 25 05 11.XX editing based on these

3-2.1 Obtaining Actual Impact Ratings

The SO, with concurrence from the AO, determines the impact levels of the control system. The SO may seek assistance from the designer in defining the functionality of the control system, the information the control system contains, and the **impact of failure of the control system.** While the SO and AO are uniquely qualified to determine the criticality of the mission in the facility, they will likely require assistance from the designer to determine the impact of the control system on the mission. For example, a critical mission of processing real-time DoD intelligence data may not depend at all on the lighting control system in the data center. For the DoD, impact levels are determined based on the mission of the relevant Service and in many cases can use the mission criticality rating of the facility (mission support, mission essential, mission critical) as a starting point to determining control system impact. It's also important to note that while a traditional information system generally prioritizes Confidentiality, then Integrity and lastly Availability, control systems usually prioritize Availability and Integrity over Confidentiality.

Note this discussion assumes that the SO and AO have been identified for the system. In many cases, this may be difficult – at this stage of the project the SO may not yet be identified. In many cases the impact of the control system is driven by the impact of the control system on the mission supported by the control system (such as a data center supported by mechanical and electrical systems) so, while the local O&M staff may “own” the control system, the impact of the control system is driven by the underlying mission supported by the control system so that the “effective” SO is a facility tenant. Ultimately, while identification of an SO and AO is not the designer's responsibility, lack of identification can present a roadblock to successful project implementation.

20

UFC 4-010-06
10 October 2023

3-2.2 When Impact Ratings Aren't Provided

If impact ratings aren't provided, request them from the Service. If the Service is unable to provide impact ratings, then request direction from the Service and follow one of the following three courses of action as directed:

1. Use one of the categorization methods discussed in APPENDIX D to categorize the system for purposes of design and document how the categorization was determined.
2. Design the system to a L-L-L impact rating.
3. Do not proceed with the design until C-I-A impact ratings are provided.

Note that these options are presented in preference order, with course of action 1 being the preferred solution. When the Service provides direction on which course of action to follow, follow that course of action. Should the Service not provide direction, use the first course of action.

3-2 STEP 1: DETERMINE CONTROL SYSTEM IMPACT RATING.

The SO, with concurrence from the AO, determines the impact levels of the control system. The SO may seek assistance from the control system designer in defining the functionality of the control system, the information the control system contains, and the impact of failure of the control system. For the DoD, impact levels are determined based on the mission of the relevant Service and in many cases can use the mission criticality rating of the facility (mission support, mission essential, mission critical) as a starting point to determining control system impact. It's also important to note that while a traditional information system generally prioritizes Confidentiality, then Integrity and lastly Availability, control systems usually prioritize Availability first, then Integrity and lastly Confidentiality.

If impact ratings aren't provided, request them from the Service. If the Service is unable to provide impact ratings then request direction from the Service and follow one of two courses of action as directed:

1. Use the “starting” impact ratings for the control system type and facility rating (mission support, mission essential, mission critical) from the Control System Master List available at the RMF Knowledge Service website (<https://rmfks.osd.mil>).
2. Do not proceed with the design until C-I-A Impact ratings are provided.

Notice New UFC has much more directions for how a Cyber Designer can “assume” C-I-A Loss of System Impact Ratings

Notice an entire Appendix has been created to instruct the Cyber Designers how to make and then “justify” these assumptions of C-I-A Loss of System Impact Ratings

Challenges Faced with “New” Version

- Control System PE Lead Designers
 - “*Don’t care*” about C-I-A Impact ratings whereas ***Cyber Designers DO!***
 - Historically work closer with end users to define their needs early in project development whereas Cyber Designers have been presumed to NOT work with end users until well after 35%
 - Historically are not familiar with why C-I-A Impact ratings may impact their control system designs whereas Cyber Designers KNOW the choices a Control System PE Lead Designer makes WILL impact the Cyber Designer’s choices if Cyber is not included from the very beginning.
 - Failure to include Cybersecurity Designers at Charrette and throughout the Design Process may result in repeat of Cyber Design work



20
24

JOINT ENGINEER
TRAINING CONFERENCE
& EXPO

SAMEJETC.ORG



@SAMENATIONAL



@SAME_NATIONAL



#SAMEJETC24



"SOCIETY OF AMERICAN MILITARY ENGINEERS"

How many paths are there?

If C-I-A Ratings not provided in RFP request from service. If service unable to provide, then *“request direction from the Service and follow one of the following three courses of action as directed:*

- 1. Use one of the categorization methods discussed in APPENDIX D to categorize the system for purposes of design and document how the categorization was determined.*
- 2. Design the system to a L-L-L impact rating.*
- 3. Do not proceed with the design until C-I-A Impact ratings are provided.”*

“Say What????”

UFC 4-010-06
10 October 2023

3-2.2 When Impact Ratings Aren't Provided

If impact ratings aren't provided, request them from the Service. If the Service is unable to provide impact ratings, then request direction from the Service and follow one of the following three courses of action as directed:

1. Use one of the categorization methods discussed in APPENDIX D to categorize the system for purposes of design and document how the categorization was determined.
2. Design the system to a L-L-L impact rating.
3. Do not proceed with the design until C-I-A Impact ratings are provided.

Note that these options are presented in preference order, with course of action 1 being the preferred solution. When the Service provides direction on which course of action to follow, follow that course of action. Should the Service not provide direction, use the first course of action.



Appendix D – Four Options to Use

1. Compare to Similar systems - ***“most defensible,” “easiest approach”*** and uses ***“established categorization values”***
2. Methodical System Review – ***“‘common sense’ approach...based on the mission and the relationship the control system has to the mission”***
3. Use the FRCS Master List – Latest Version is 2021
4. Use the National Institute of Standards and Technology (NIST) Guidance – ***“the ‘proper formal way’”***

D-2 SYSTEM CATEGORIZATION AND DETERMINATION OF IMPACT RATING

Step 1 of the RMF requires categorizing the system in accordance with Committee on National Security Systems Instruction (CNSSI) 1253. This instruction describes how the CIA impact level is determined by the type of information on the system and mission criticality of the system. Rationales for system categorization will be required and may be supported by four approaches (listed in order of preference):

1. Compare to Similar Systems. This is probably the most defensible and easiest approach; is the project similar to an existing project with established categorization values?
2. Methodical System Review. This is a “common sense” approach to determining impact ratings based on the mission and the relationship the control system has to the mission.

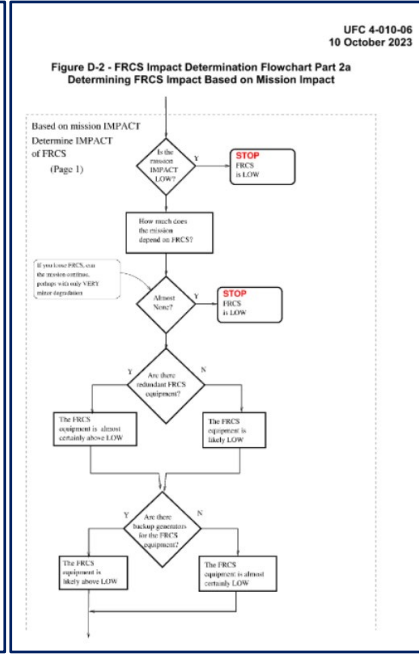
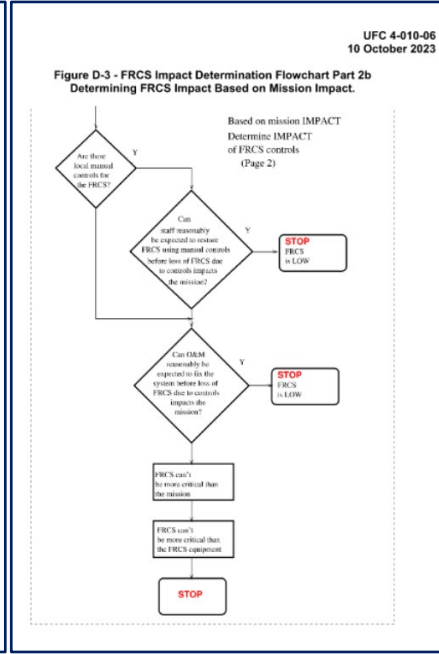
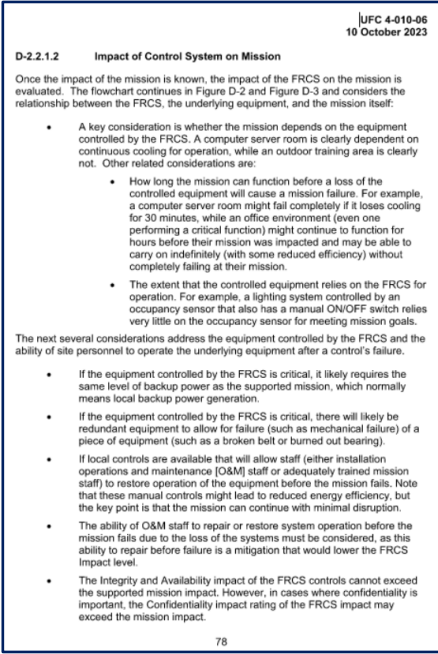
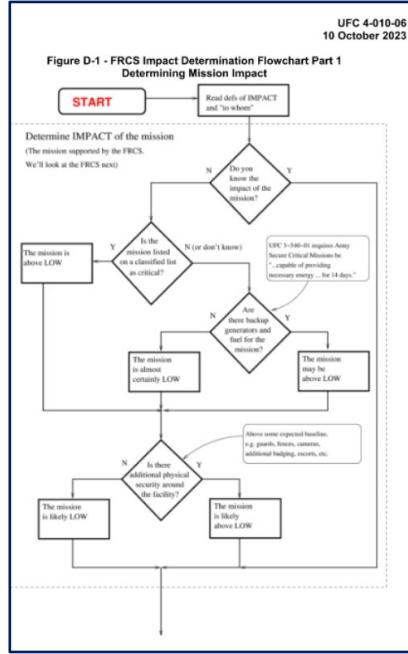
74

UFC 4-010-06
10 October 2023

3. Office of the Assistant Secretary of Defense for Sustainment (Energy, Installations and Environment) FRCS Master List (https://www.acq.osd.mil/eie/IE/FEP_CSC.html). This list includes “starting point” CIA impact ratings by control system type for three mission criticalities. The values here have generally (and more specifically for Utility Monitoring and Control System (UMCS), BCS, and UCS) been determined through an application of the “common sense” methodical process defined here.
4. National Institute of Standards and Technology (NIST) Guidance. This is the “proper formal way” to determine impact ratings but is not easily applicable to control systems. In practice, the approach used is to determine CIA using another approach first and then to confirm/document that impact rating determination using the NIST guidance.



“So, what do I do again?”

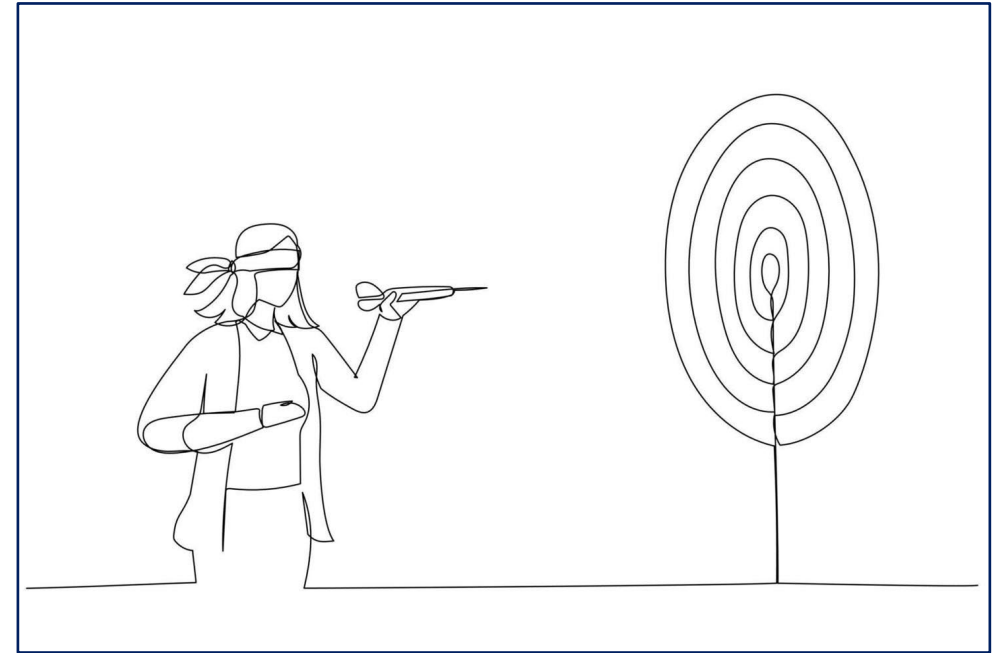


Methodical System Review – **“common sense (???) approach... based on the mission and the relationship the control system has to the mission”**

“State Your Impact Rating Assumptions”

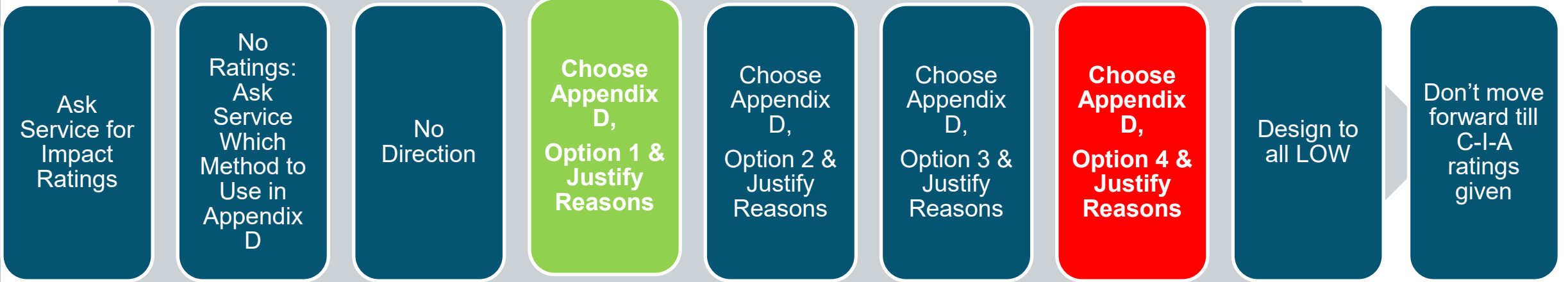
Chapter 3, Section 3-2.2 When Impact Ratings Aren't Provided:

“When the Service provides direction on which course of action to follow, follow that course of action. Should the Service not provide direction, use the first course of action.”



What this looks like in Real Life

Most Difficult & Time Consuming for Cyber Designer



Easiest for Cyber Designer IF THEY ARE INVOLVED FROM THE BEGINNING!

Justify Your Reasons/Assumptions

Example (Compare to Existing System(s): “Per the Statement of Work, Section C, the existing Fire Alarm and Mass Notification System (FAMNS) is to be demolished and replaced with a new FAMNS. Therefore, Cybersecurity Design shall assume that the Loss of System Impact Ratings for the new FAMNS shall be the same as the existing system which is to be demolished.”

Set Time Period For Assumptions

Example: “Upon completion of the 35% Design Review by the client, if the assumed C-I-A Loss of Control System(s) Impact Rating design requirements have not been confirmed by the client, then the Cybersecurity Design for the FRCS identified will continue based on these assumptions presented to ensure the design stages of the Cybersecurity Design Process listed in Chapter 5, section 5-4, REQUIREMENTS BY DESIGN PHASE, are met.”

Live Content Slide

Poll: True or False: Once the C-I-A Impact Rating(s) is/are determined or assumed, that's all that is needed to move forward for the Cybersecurity Design Process as laid out in UFC 4-010-06?

Oh! Wait! There's More!

- Use of Overlay for the C-I-A Impact Ratings Affects Cyber Design for the Control System
- 3-3.2.2 Identifying An Appropriate Overlay *“Based on the Service, project site and control system type there are several different overlays that may apply...”*

3-3.2.2 Identifying An Appropriate Overlay

Based on the Service, project site and control system type there are several different overlays that may apply, including:

- NIST SP 800-82
- The Control System Overlay for Moderate Impact Systems published by the Risk Management Framework Technical Advisory Group (RMF TAG Overlay)
- (NAVY) The Navy Assess-Only Overlay
- (AIR FORCE) The Air Force Control System Overlay

When the Service does not provide a specific overlay, use NIST SP 800-82 or the RMF TAG Overlay (or a combination) to define the control set for design based on the C-I-A Impact Ratings:

- For a system with L-L-L Impact ratings: Use NIST SP 800-82.
- For a system with M-M-M Impact ratings: Use the RMF Tag Overlay

⁶ Imagine a L-M-M system using a M-M-M table that includes a control that states “Sensor values must be protected against unauthorized disclosure”. CNSSI 1253 indicates that this control is for C. Consult the corresponding L-L-L table and see if the control is required, if not, it may be removed from consideration.

23

UFC 4-010-06
10 October 2023

- For a system with a mix of Impact Levels (such as L-M-M), use CNSSI 1253 to determine – for each control – which element of the CIA triad (the Confidentiality, Integrity or Availability) that control applies to. Then determine applicability of the control based on the assigned impact levels using the appropriate overlay:
 - For Low impact elements, use NIST 800-82
 - For Moderate impact elements, use the RMF TAG Overlay
 - For High impact elements, use both NIST 800-82 and the RMF TAG Overlay and include controls in the baseline if they are included by either overlay.

As described in the next paragraph, there are tables in the UFC that use these overlays with a high-water mark, and an Excel tool that can be used for systems with a mix of Impact Levels.

Lessons Learned – Objective 1: The RFP

- Involve Cybersecurity SMEs very early when pursuing (A-Es) or writing (Government) an RFP
- UFC 4-010-06 does NOT execute the Risk Management Framework & Does NOT Provide an ATO; It allows the Control System to be more “ATO Ready”
- Words Matter! Read the RFPs Carefully! Get the Cyber SME to review it!
- Be Prepared to Ask a LOT of RFIs

Lessons Learned – Objective 2: Costs

- There are Direct (e.g., Impact Ratings, # of Control Systems, Types of Control Systems etc.) and Indirect Variances (e.g., Attendance of Cybersecurity Designer at the Charrette, Attendance of ISSO/ISSM, working with PEs from the A-E & Government etc.) for Costs
- There are Build and Implementation Costs
- These require coordinating Contractor Submittals is paramount to keeping costs DOWN
- This is done by close coordination between Cybersecurity Designer, PEs Designing the Systems and Government ***during the design phase first BEFORE*** the building and implementation phases

Lessons Learned – Objective 3: Design Phases

- New UFC 4-010-06 dictates specific requirements to be delivered at each design issuance
- There are “**New Contractor**” *Cybersecurity Design Coordination Questions To Answer*
- There are “**New MODERATE**” *Cybersecurity Design Coordination Questions To Answer*
- There is an expectation that the Cybersecurity Designer will work closely with the PEs Designing the Control Systems and coordinate this with the Government Clients
- None of this “**NEW;**” It has always been expected, now its just being enforced

Lessons Learned – Objective 4: Ratings/Overlay Assumption

- New UFC 4-010-06 Allows for Cybersecurity Designer to “**Assume**” Loss of System Impact Ratings for Control Systems in the project
- This means the Overlays AND the C-I-A Impact Ratings must be justified by the Cybersecurity Designer
- There is an expectation that the Cybersecurity Designer will work closely with the PEs Designing the Control Systems and coordinate this with the Government Clients to make, and then justify, these assumptions

The New UFC 4-010-06 of 2023:
A Practical Breakdown

THANK YOU

Please take a few minutes to complete a short survey about this session. Your feedback will help us improve future programming for JETC.

 **conferences** i/o



or browse to
jetc.cnf.io

The New UFC 4-010-06 of 2023: A Practical Breakdown

Q&A

- Presenter:
F. Charlene Watson, charlene.Watson@hdrinc.com
- Moderator:
Lori Jackson, lori@whiteravensecurity.com