Society of SAME American Military Engineers Orange County Post

Michael Baker INTERNATIONAL

# APRIL 18TH 2024 LUNCHEON
# FRCS CYBERSECURITY AND THE NEW UFC 4-010-06

## Featuring Jim Sullivan, NAVFAC SW CIO

## Panelists from HDR and Michael Baker International

HDR

NAVFAC Naval Facilities Engineering Systems Command NAVFAC Southwest

Naval Facilities Engineering Systems Command
NAVFAC Southwest

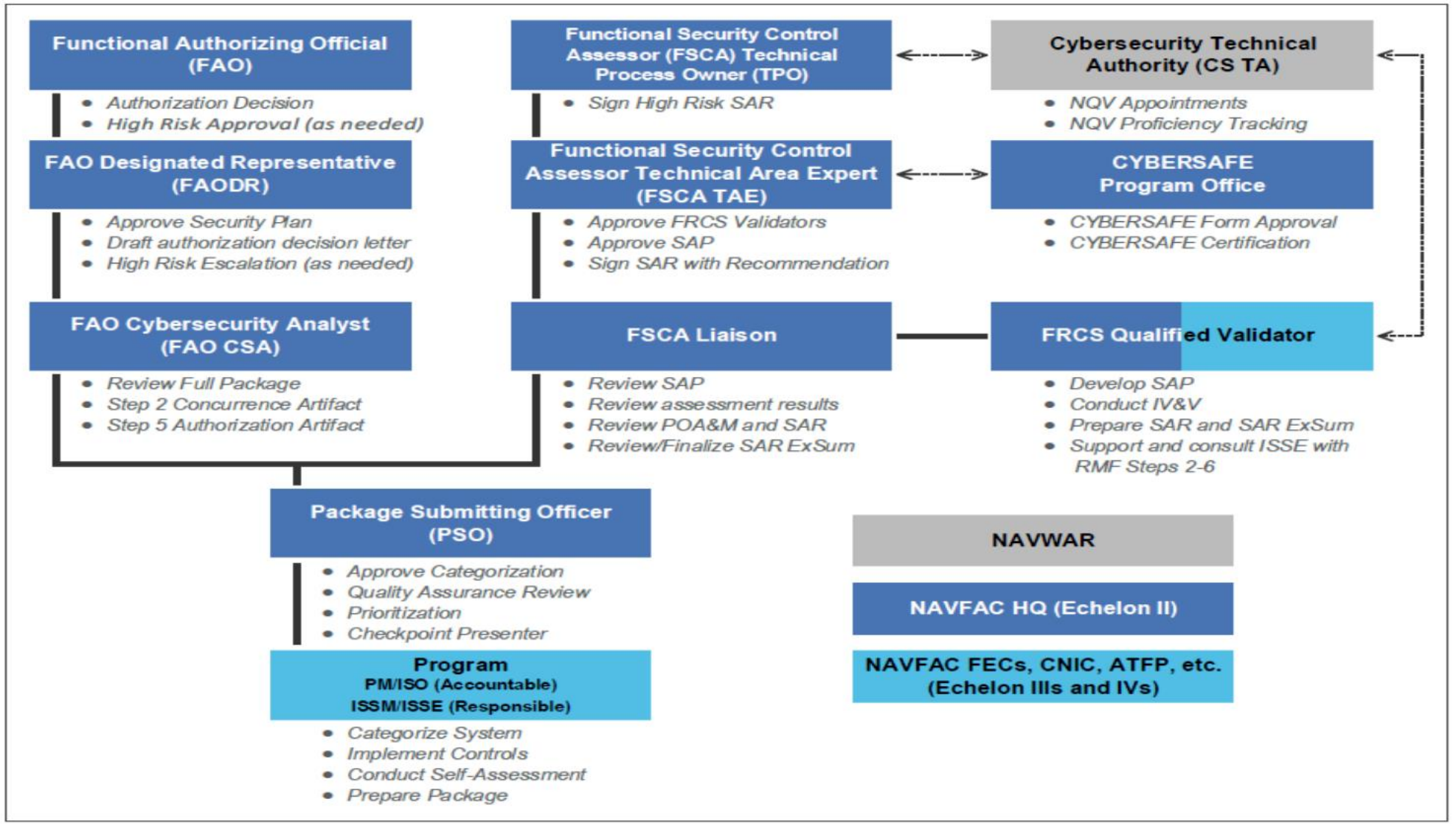
# NAVFAC SW CIO
# Cybersecurity Commissioning (CyCx)

SAME Luncheon

*18 Apr 2024*

Society of SAME American Military Engineers Orange County Post

# RMF Roles


Functional Authorizing Official (FAO)
Authorization Decision
High Risk Approval (as needed)
FAO Designated Representative (FAODR)
Approve Security Plan
Draft authorization decision letter
High Risk Escalation (as needed)
FAO Cybersecurity Analyst (FAO CSA)
Review Full Package
Step 2 Concurrence Artifact
Step 5 Authorization Artifact
Functional Security Control Assessor (FSCA) Technical Process Owner (TPO)
Sign High Risk SAR
Functional Security Control Assessor Technical Area Expert (FSCA TAE)
Approve FRCS Validators
Approve SAP
Sign SAR with Recommendation
FSCA Liaison
Review SAP
Review assessment results
Review POA&M and SAR
Review/Finalize SAR ExSum
Cybersecurity Technical Authority (CS TA)
NQV Appointments
NQV Proficiency Tracking
CYBERSAFE Program Office
CYBERSAFE Form Approval
CYBERSAFE Certification
FRCS Qualified Validator
Develop SAP
Conduct IV&V
Prepare SAR and SAR ExSum
Support and consult ISSE with RMF Steps 2-6
Package Submitting Officer (PSO)
Approve Categorization
Quality Assurance Review
Prioritization
Checkpoint Presenter
Program
PM/ISO (Accountable)
ISSM/ISSE (Responsible)
Categorize System
Implement Controls
Conduct Self-Assessment
Prepare Package
NAVWAR
NAVFAC HQ (Echelon II)
NAVFAC FECs, CNIC, ATFP, etc. (Echelon IIIs and IVs)

# Key RMF Roles

- FAO - Exclusively responsible and accountable for FRCS-related security risks. Makes an authorization decision based on the FRCS-related security risks that may impact organizational operations and assets, individuals, other organizations, or the Nation.

- FSCA Liaison - Acts as the FSCA TAE's direct representative. The FSCA Liaison is considered a risk assessment Subject Matter Expert

- Validator - Acts as an independent third party who assesses and validates that the system has implemented the approved security control baseline. The Validator acts as a trusted agent to the FSCA.

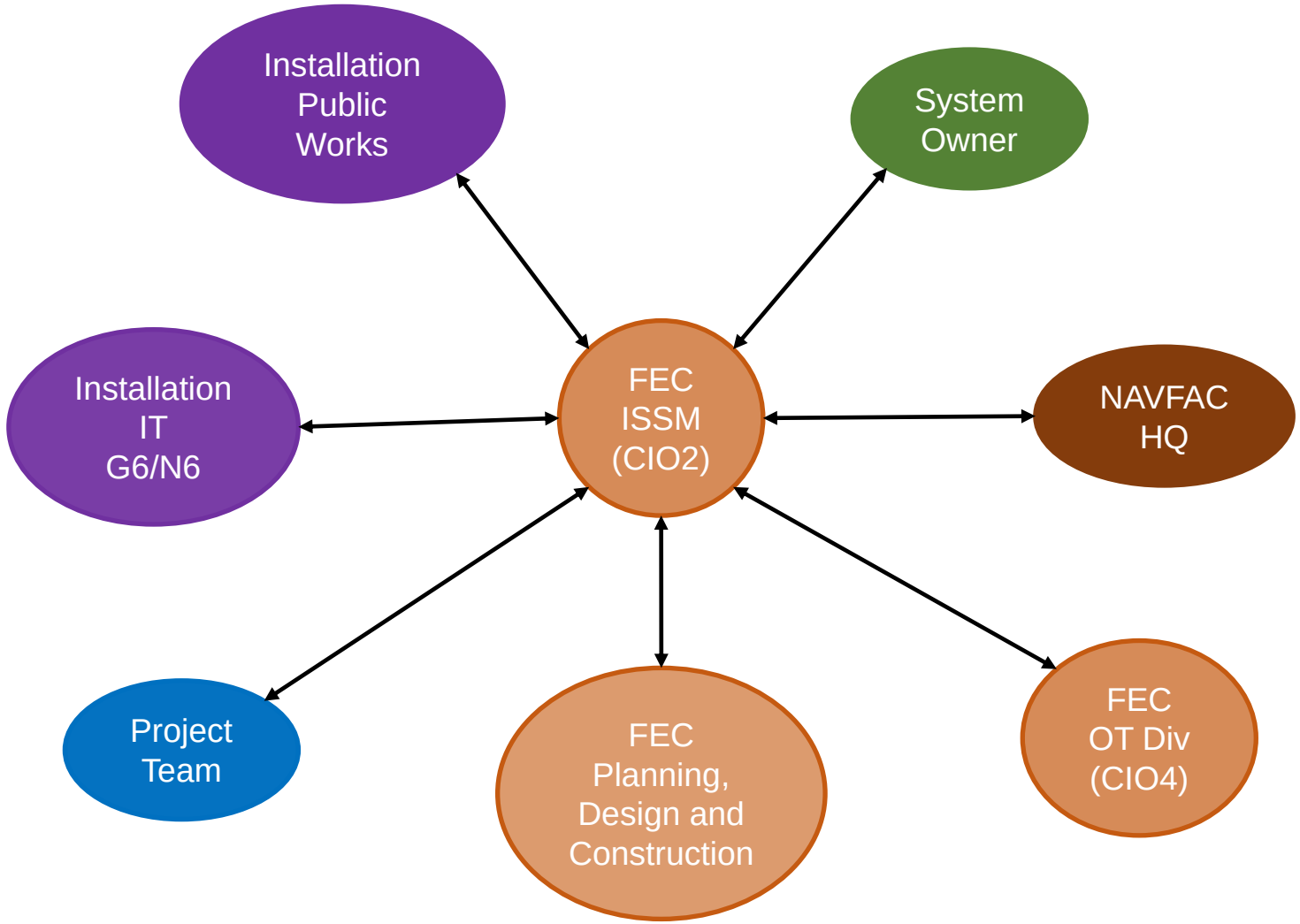
- PSO - Responsible for prioritizing, enforcing standardization, and performing quality assurance reviews prior to establishing Checkpoints.

- ISSM - Responsible for the cybersecurity of a program, organization, system, or enclave, and is accountable to the PM/ISO.

- The PM/ISO - Shares the responsibility and authority to accomplish funded and allocated program- or system-objectives for development, production, acquisition, and sustainment to meet Navy operational needs.

Society of SAME American Military Engineers Orange County Post

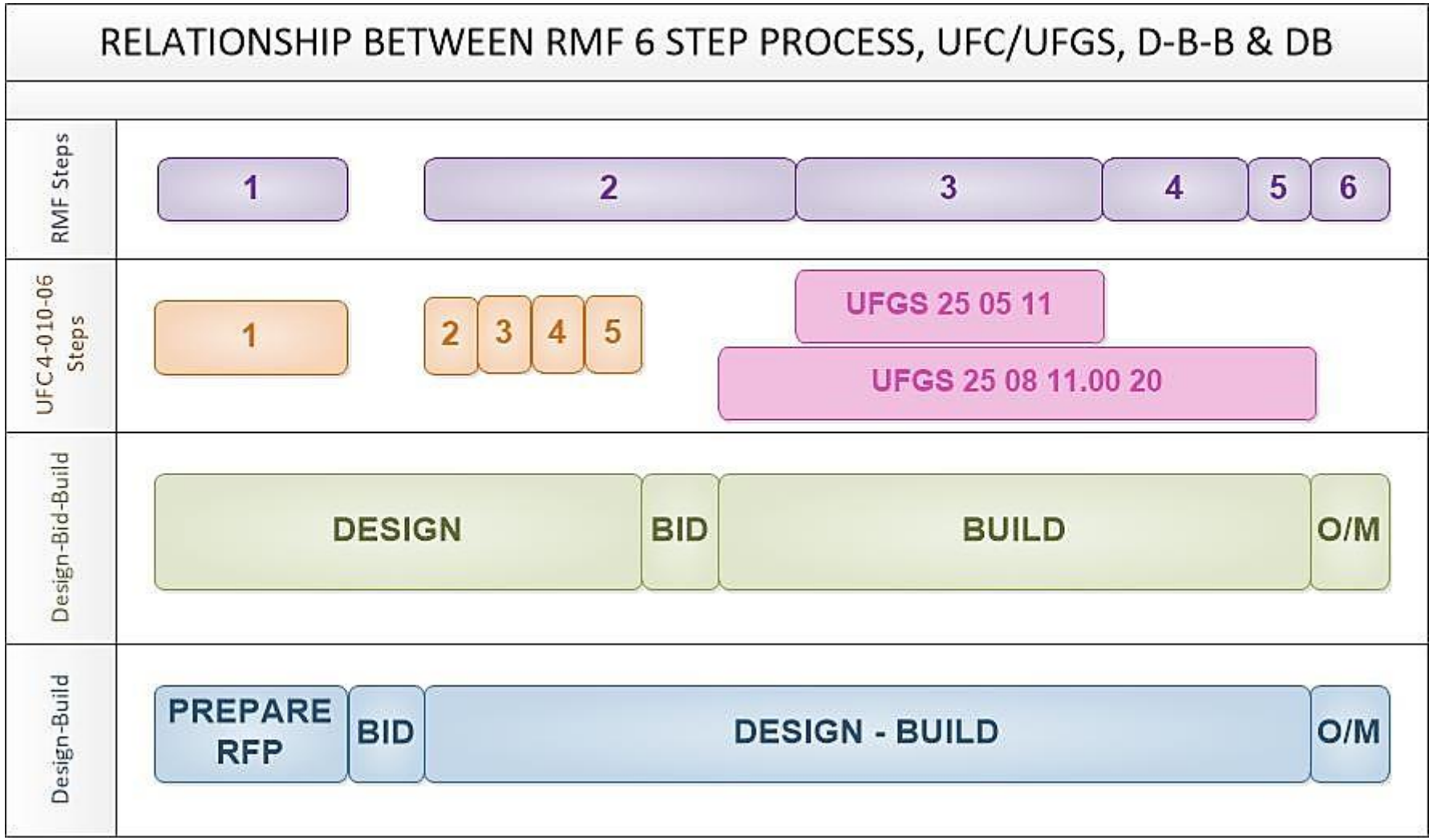
# ISSM Relationships



# Risk Management Framework Steps

1. Categorize System
2. Select Controls
3. Implement Controls
4. Assess Controls
5. Authorize System
6. Continuous Monitoring

# RMF vs. DB/DBB


RELATIONSHIP BETWEEN RMF 6 STEP PROCESS, UFC/UFGS, D-B-B & DB
RMF Steps
1
2
3
4
5
6
UFC 4-010-06 Steps
1
2
3
4
5
UFGS 25 05 11
UFGS 25 08 11.00 20
Design-Bid-Build
DESIGN
BID
BUILD
O/M
Design-Build
PREPARE RFP
BID
DESIGN - BUILD
O/M

# Cybersecurity Strategies

- **Authorization to Operate (ATO)**
  - An ATO is a full system cybersecurity assessment and authorization using the Risk Management Framework (RMF) process. The Commander, NAVFAC signs ATOs as the functional Authorizing Official for Facility-Related-Control Systems. The requirements are documented in the NAVFAC Echelon II Risk Management Framework (RMF) Business Rules.*
- **Memorandum for the Record (MFR)**
  - A MFR is a way of documenting a change to a system, such as adding equipment. MFRs are system baseline changes impacting a system with an existing ATO. Change requests are submitted to the Change Control Boards (CCB).
- **Unified Facility Guide Specifications (UFGS) 25 05 11**
  - The UFGS 25 05 11 requires implementation of some control requirements supporting but not requiring the full RMF process. It will be used when adding equipment to systems that cannot be authorized through the MILCON project. UFGS 25 05 11 consolidates all cybersecurity submittals into one specification.

# Sample FRCS Cybersecurity Strategies

| Control System | CIA Rating | Connection Strategy | Cybersecurity Strategy |
|---|---|---|---|
| HVAC Direct Digital Control | M-M-M | Connect to base-wide system | UFC 4-010-06 + UFGS 25 05 11 + MFR |
| Utility Metering | M-M-M | Connect to AMI | MFR |
| Water Treatment Plant | L-L-L | Connect to CSPE | UFC 4-010-06 + UFGS 25 05 11 + UFGS 25 08 11 + ATO |
| Fire Detection and Alarm | L-M-M | N/A | N/A |

# General Thoughts

- **Start with IDing FRCS and understanding strategy**
- **Goal should be "Connectable" and "Authorizable"**
  - **Connectable to existing system and/or CSPE**
  - **"Authorizable"**
    - ATOs are not common
    - Project should deliver system/components that can be authorized
- **Understanding CIA and how it impacts the project**
  - **Can project meet required levels**
- **System SOPs**
  - **Clear understanding of who is responsible based on CCIs**
- **Submittals/Deliverables**
  - **What is required, interfaces**
- **Understanding how to address controls, even if they can't be met**
- **Engage with ISSM POC**
  - **Ask for us if you don't see us involved (COR)**
  - **Ask questions**

# FRCS CYBER AND THE PROJECT DESIGN CHARRETTE

*Susan Howard*
*VP ICS/OT Cybersecurity*
*Michael Baker International*

## FRCS CYBERSECURITY IS TRULY A TEAM SPORT

Society of SAME American Military Engineers Orange County Post

NAVFAC Naval Facilities Engineering Systems Command NAVFAC Southwest

# FRCS CYBER AND THE PROJECT DESIGN CHARRETTE

**FRCS CYBERSECURITY STAKEHOLDERS INCLUDE BUT NOT LIMITED TO THE FOLLOWING THAT SHOULD BE AT DESIGN CHARRETTES. Project Management Team to ensure these stakeholders are present:**

- Architects
- Engineers – Electrical, Mechanical, Fire, Controls, Water & Others
- Contractors – General Contractors, Commissioning (CxA's)
- Owners – System Owners, Owner Reps, Design and Project Managers
- Facility Managers – Public Works Dept (PWD), Dept of Public Works (DPW), Civil Engineering Squadrons
- Maintenance Engineers
- Physical Security Specialists – ESS (CCTV, Intrusion Detection etc.)
- Information Assurance Professionals – NAVFAC, AFCEC, and USACE Information Systems Security Managers (ISSMs), NAVFAC CIO2/CIO4

# THE PROJECT DESIGN CHARRETTE
# Estimated Duration of Discussion is 2 HOURS for FRCS Cyber ONLY

- Sample Agenda and Question Set for Charrette on Next Slide
- Could require as many as 20 stakeholders to answer during charrette – Be Prepared
- 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 DESIGN CHARRETTE AGENDA FOR FRCS CYBERSECURITY

1. **Validate which control systems will be included – requires all engineering stakeholders present:**
   - Fire Systems – will they be IP based?
   - HVAC Building Control Systems – will these be connected to an existing basewide Front End?
   - Electrical systems – Lighting, Generators, Substations, Microgrid systems, others?
   - Cranes – YES – Cranes require cybersecurity especially on NAVFAC projects www.whitehouse.gov/administration-announces-initiative-to-bolster-cybersecurity-of-u-s-ports/
   - Water treatment systems
   - Elevators
   - 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?**

# NAVFAC ASHORE CYBER FRAMEWORK

## START HERE

NAVFAC's Cyber Security mission is to safeguard thousands upon thousands of Industrial Control Systems (ICSs) that serve to maintain and operate a vast real property inventory:

- Buildings: 87,000+
- Structures: 52,000+
- Linear Structures: 21,000+
- Special Areas: 900+

This effort is further complicated by the fact that these "Systems of Systems" are geographically dispersed around the globe.

## CYBER SECURITY POLICIES & MANDATES

**Executive Order (EO) 13636:** Improving Critical Infrastructure Cyber Security

**Presidential Policy Directive (PPD) 21:** Critical Infrastructure Security and Resilience

**NIST Guide to Industrial Control System(s) Security (NIST) 800-82:** Framework—refined from existing standards, guidelines, and practices—for reducing Cyber Risks to Critical Infrastructure

**DoDI 8500:** DoD Cyber Security Program

**DoDI 8510:** Risk Management Framework (RMF) for DoD Information Technology (IT)

**Draft DoDI 8530:** Department of Defense Computer Network Defense

**Draft DoDI 8140:** Cyberspace Workforce Guide

**CNSSI 1253:** Security Categorization and Control Selection for National Security Systems

**CYBER HYGIENE - ALL HANDS ON DECK**

## DEFENSE IN DEPTH FUNCTIONAL IMPLEMENTATION ARCHITECTURE (DFIA)

- POLICIES & PROCEDURES
- PHYSICAL DEFENSES
- PERIMETER DEFENSES
- NETWORK DEFENSES
- HOST DEFENSES
- APPLICATION DEFENSES
- DATA DEFENSES

## TECHNICAL AUTHORITY MISSION AREAS

- FACILITIES
- ANTI TERRORISM & FORCE PROTECTION (ATFP)
- UTILITIES
- ENVIRONMENTAL
- WEIGHT HANDLING
- EXPEDITIONARY

## RISK MANAGEMENT FRAMEWORK (RMF)


## THREATS

**FOREIGN NATION STATES**
Typically the most skilled and dangerous type of Hackers—Foreign Nation States seek to gain intelligence on or cause serious harm to the people and interests of the United States.

**CYBER MERCENARIES**
Skilled and out for personal gain—Cyber Mercenaries may operate independently, as a group, or hired in part of a larger Foreign Nation State effort.

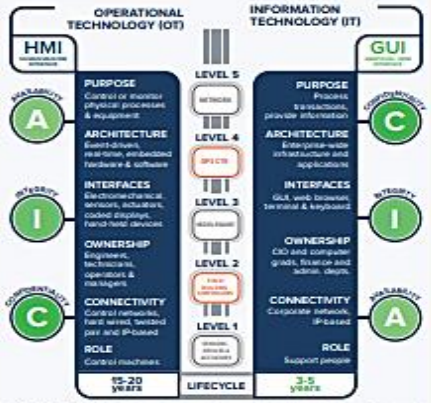
**HACKTIVISTS**
Often considered as "cyber-vigilantes seeking political ends," Hacktivists typically seek to coordinate attacks that create discourse by garnering major media focus.

**SCRIPT KIDDIES**
These cyber-criminals typically use existing malware to attack systems for the purpose of vandalism or in order to gain personal notoriety.

## TYPES OF MALWARE

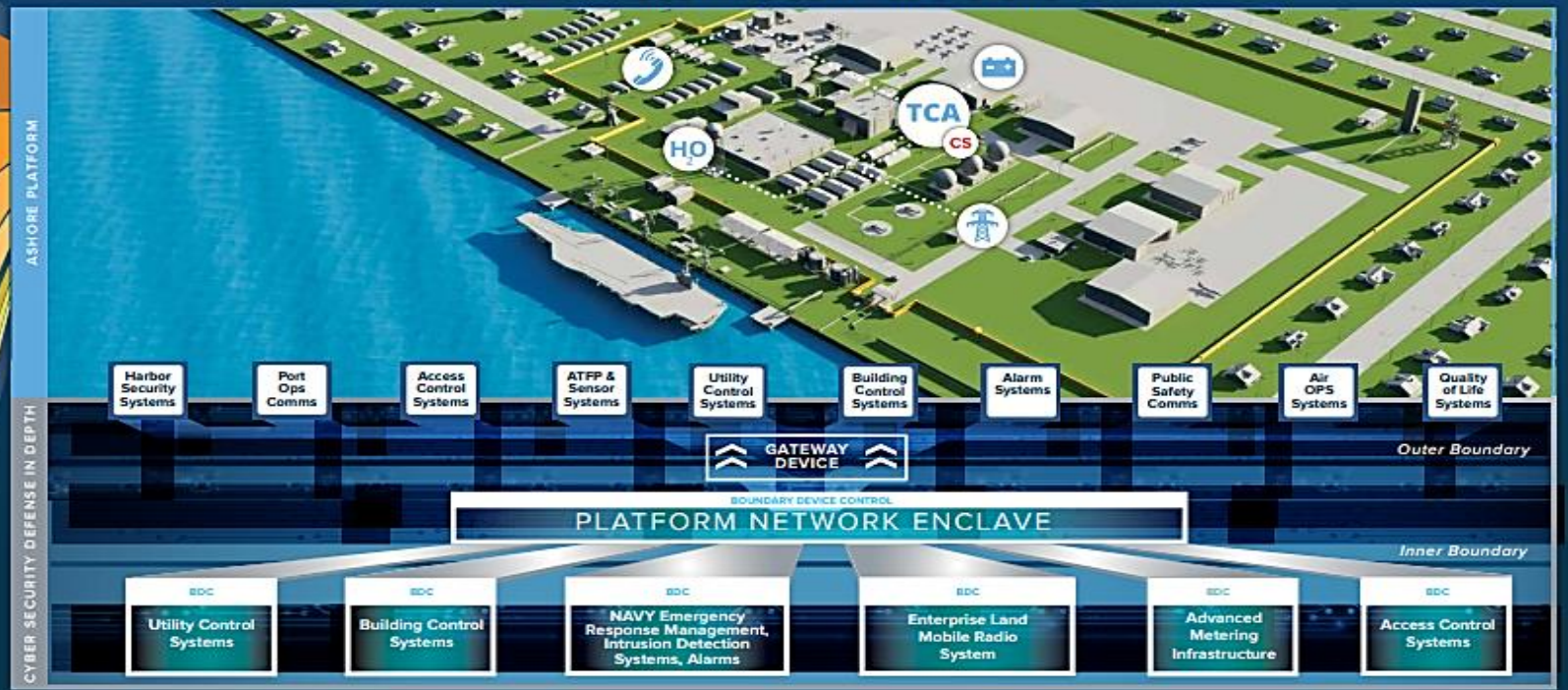
- BLACK ENERGY/ DUQU
- DUQU/ FLAME
- OPERATION CLEAVER

## CHALLENGES




CNSSI No. 1253 (Security Control Overlays For Industrial Control Systems)

## NAVY INDUSTRIAL CONTROL SYSTEMS




## RISK MANAGEMENT PROGRAM


## CYBER SECURITY AND CYBERSAFE PROCESSES


## TASK FORCE CYBER AWAKENING (TFCA):

**Holistic View:**
Gaining the insight to conquer uneven and fragmented Cyber Security efforts across Navy platforms and systems.

**Cyber Awareness:**
Communicating Cyber Security methodologies across the Navy to overcome disparate levels of Cyber Awareness.

**CYBERSAFE:**
To provide maximum reasonable assurance of a hardened subset of critical warfighting components and processes.

## NAVFAC CYBER WORKFORCE:

**Subject Matter Expertise:**
Cultivating a multi-disciplinary workforce and mindset, integrating Cyber Security and domain expertise, in order to enable mission assurance.

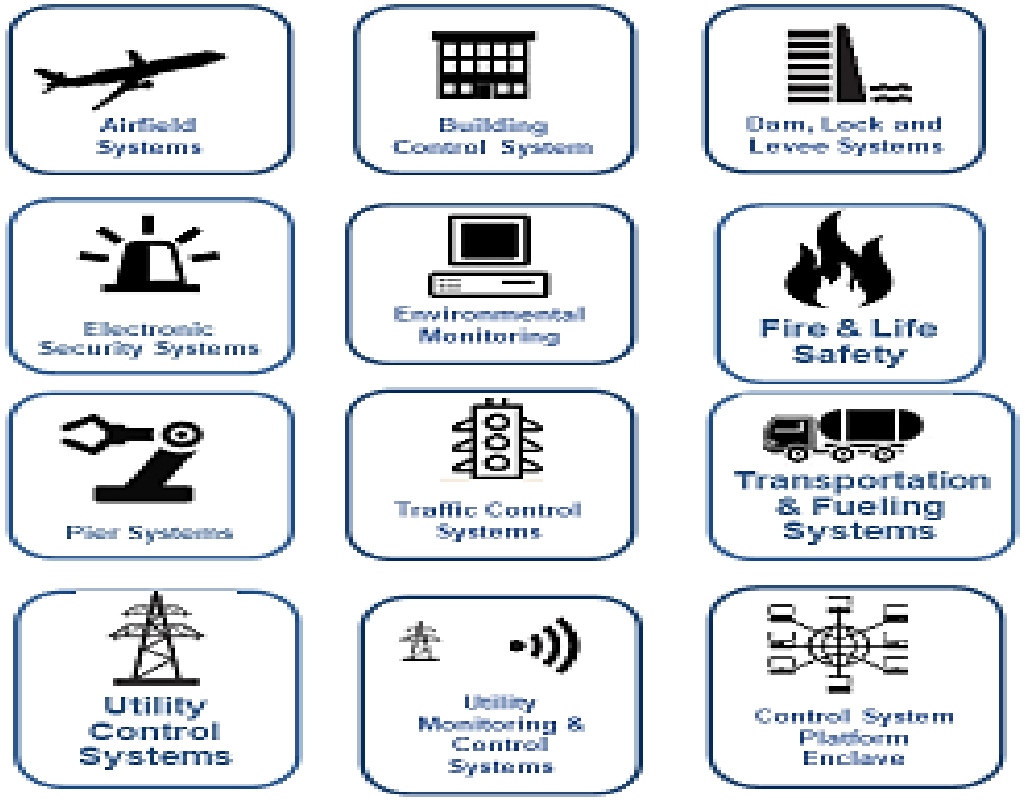
PEOPLE & RESOURCES

V 09 MAY 2015

# THE PROJECT DESIGN CHARRETTE
# THINK YOU DON'T NEED CYBER? THINK AGAIN

## DoD Facility-Related Control Systems (FRCS)

### Categories




### Systems

- Building Automation System
- Building Lighting System
- Conveyance/Vertical Transport System
- Electrical Systems
- Heating, Ventilation, Air Conditioning
- Irrigation System
- Shade Control System
- Vehicle Charging System
- Cathodic Protection Systems
- Compressed Air (Or Compressed Gases) System
- Central Plant (District) Chilled Water System
- Central Plant (District) Electrical Power Production
- Central Plant (District) Hot Water System
- Central Plant (District) Steam System
- Electrical Distribution System
- Gray Water System
- Industrial Waste Treatment System
- Microgrid Control Systems
- Natural Gas System
- Oily Water/Waste Oil System
- Potable Water System
- Pure Water System
- Salt Water System
- Sanitary Sewer/Wastewater System
- Utility Metering System (Advanced Meters, AMI, etc.)
- *Many More…*

**DoD Control Systems are just as vulnerable as industry, how do we protect them?**

# WANT TO KNOW MORE?
# CHECK OUT THE WBDG WEBSITE CYBER RESOURCE PAGE
## https://www.wbdg.org/resources/cybersecurity

WBDG Whole Building Design Guide

LOGIN CREATE ACCOUNT SEARCH

DESIGN RECOMMENDATIONS | PROJECT MANAGEMENT - O & M | FEDERAL FACILITY CRITERIA | CONTINUING EDUCATION | ADDITIONAL RESOURCES

RESOURCE PAGES / CYBERSECURITY

# Cybersecurity

*by Michael Chipley PhD, PMP, LEED AP*
*The PMC Group LLC*

**Updated:** 02-21-2020

## INTRODUCTION

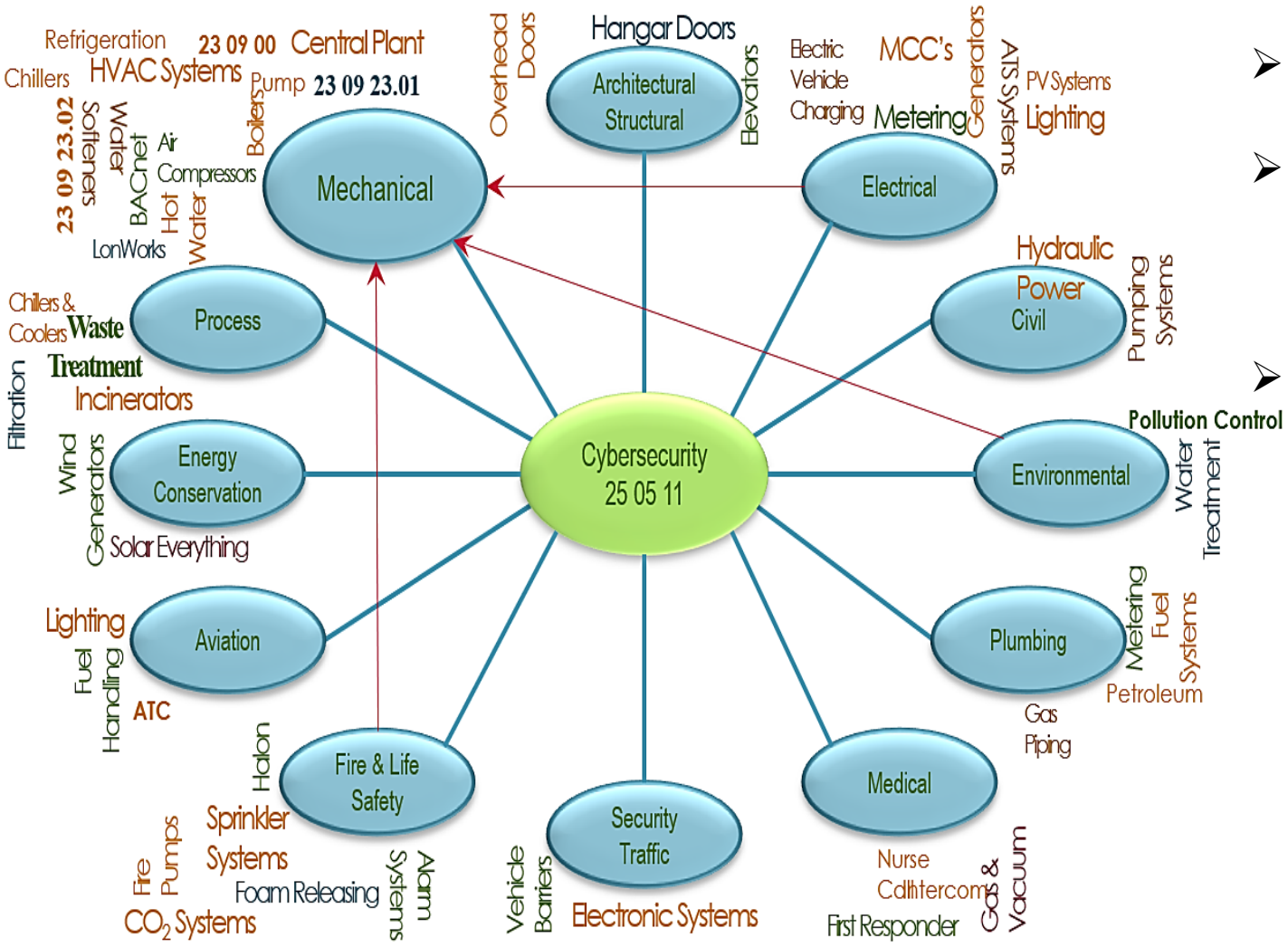
Industrial Control Systems (ICS) are physical equipment oriented technologies and systems that deal with the actual running of plants and equipment, include devices that ensure physical system integrity and meet technical constraints, and are event-driven and frequently real-time software applications or devices with embedded software. These types of specialized systems are pervasive throughout the infrastructure and are required to meet numerous and often conflicting safety, performance, security, reliability, and operational requirements. ICSs range from building environmental controls (HVAC, lighting), to systems such as the electrical power grid. With the increasing interconnectivity of ICS to the internet, the ICS can be an entry point into the organization's other IT systems.

*WITHIN THIS PAGE*

- Introduction
- Description
- Additional Resources

Society of SAME American Military Engineers Orange County Post

# FRCS Cybersecurity




- Cybersecurity is a team sport
- Interdisciplinary Partners Must be Engaged
- Early Engagement Controls Risks
  - Pursuit / Task Order
  - Charrette
- Cyber 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.

Society of SAME American Military Engineers Orange County Post

# What Projects Require the New UFC 4-010-06?

- All Projects being designed using the Unified Facilities Criteria 1-200-01:
  - Section 1-3.1 Implementation, Administration, and Enforcement states:

*"UFC and their referenced codes and Criteria are effective upon issuance for projects as follows:*

*Design-Bid-Build projects that have not proceeded beyond 35% design completion.*

*Design-Build projects that have not proceeded beyond date of Request for Proposal (RFP) issuance. When an RFP is issued in multiple phases or steps use the date of the last phase of the RFP issuance."*

- Section 1-6.3.1.1 Core UFC

*"Core UFC are criteria that provide requirements for the majority of traditional building systems that are prevalent on DoD facility construction projects. Core UFC also identify additional criteria such as Antiterrorism, High Performance, and Sustainable Building requirements mandated by law and policy. Comply with the Core UFC listed here."*

*.....*

*4-010-06 Cybersecurity of Facility Related Control Systems"*

# What Is the Difference in the New UFC 4-010-06?



**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 CCIs 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/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.



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



**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 CCIs 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)

# What Is the Difference in the New UFC 4-010-06?



**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.



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 does not even START to list what is due for the Design Issuance Yet



The recommended format for this submittal is to use the format of \1\0/1/ 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.

# What Is the Difference in the New UFC 4-010-06?



**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:





    - ◊ 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.



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"

# Normal Cyber 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?

# New Contractor Cyber Design Coordination Questions

- 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?

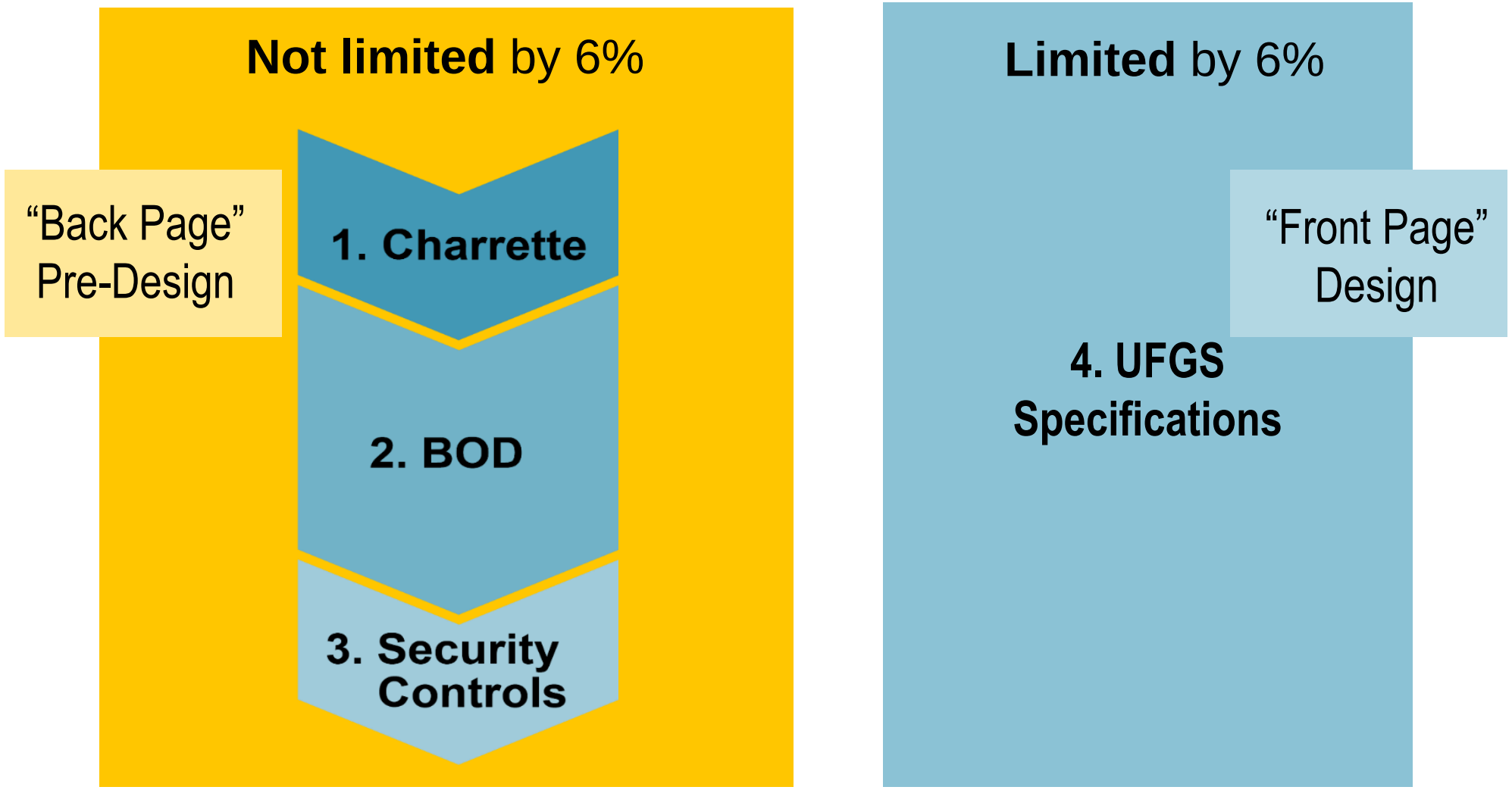
# New Cyber Design Coordination for MODERATE Control Systems

- 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?

# 04 Costs

Society of SAME American Military Engineers Orange County Post

# Federal/DoD – 6% Fee Limitation



# DoD – SCOPE / BUDGET Causes for Variance in DESIGN

- **Direct Impact:**
  - Mission Rating (Support / Essential / Critical)
  - Number of Asset Groups (HVAC, FLS, etc)
  - Asset CIA and Mission Ratings (L, M, H)
  - Connectivity or Provision of a Front-End System

- **Indirect Impacts:**
  - Charrette Attendance by Client ISSM
  - Charrette Attendance by AE Cybersecurity Designer
  - Lack of coordination efforts between Engineers, Cybersecurity Designer, and Client's Control System Owner/Operator
  - RFI Response Timeliness / Accuracy from Client

# 25 05 11 Contractor Submittals – Per FRCS System

*SD-01 Preconstruction Submittals*

- *Wireless & Wired Communications Broadcast Request*
- *Device Account Lock Exception Request*
- *Multiple IP Connection Device Request*
- *Contractor Computer Cyber Compliance*
- *Temp Contractor Computer Cyber Compliance*
- *Cybersecurity Interconnection Schedule*
- ***Protection of Information at Rest Proposal***
- ***Proposed STIG & SRG Applicability Report***
- *Qualifications*

*SD-02 Shop Drawings*

- *Network Communication Report*
- *Cyber Riser Diagram*

*SD-03 Product Data*

- *Control System Cyber Documentation*

*SD-06 Test Reports*

- *Wireless Communications Test Report*
- ***Control System Cybersecurity Testing Procedures***
- ***Control System Cybersecurity Testing Report***

*SD-07 Certificates*

- *Software Licenses*

*SD-11 Closeout Submittals*

- *Confidential Password Report*
- ***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***

# 25 08 11.00 20 Cyber Commissioning (NAVY Only)

*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 Report*
- *ISSE Checklist Step 3*
- *ISSE Checklist Step 4*

*SD-07 Certificates*
- *Information Assurance Technical Level II/Security Plus*

*Per System Non-Submittal Activity*
- *Execute SCAP*
- *ACAS Vulnerability Scans*
- *STIG Checklists*
- *POA&M Documentation*
- *SCA-V Site Assessment*
- *RMF Step 2 CheckPoint Meeting*
- *RMF Step 2 - Submittal Uploads (5 Submittals)*

*Per Project Non-Submittal Activity*
- *CAC Registration*
- *Construction Coordination Meeting*

# 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

# PANEL QUESTIONS FOR DISCUSSION

## *Charlene Watson, HDR*

**Question 1** – How can we get better designs and submittals from Contractors?

# PANEL QUESTIONS FOR DISCUSSION

## *Susan Howard, Michael Baker Intl*

**Question 2** - How can NAVFAC SW CIO better assist A&E community (GCs or Designers)?

# PANEL QUESTIONS FOR DISCUSSION

## *David Brearley, HDR*

**Question 3** - Describe common cybersecurity findings with equipment submittals (i.e. not the Div 25 submittals)? – i.e. another discipline approves hardware that doesn't meet Div 25 requirements

# THANKS SO MUCH!

**Contact Information**

Susan Howard, HDR
Susan.Howard@Mbakerintl.com

David Brearley, HDR
David.Brearley@HDR.com

Charlene Watson, HDR
Charlene.Watson@HDR.com

NAVFAC SW CIO FRCS MILCON Projects
navfac-sw-cycx@us.navy.mil