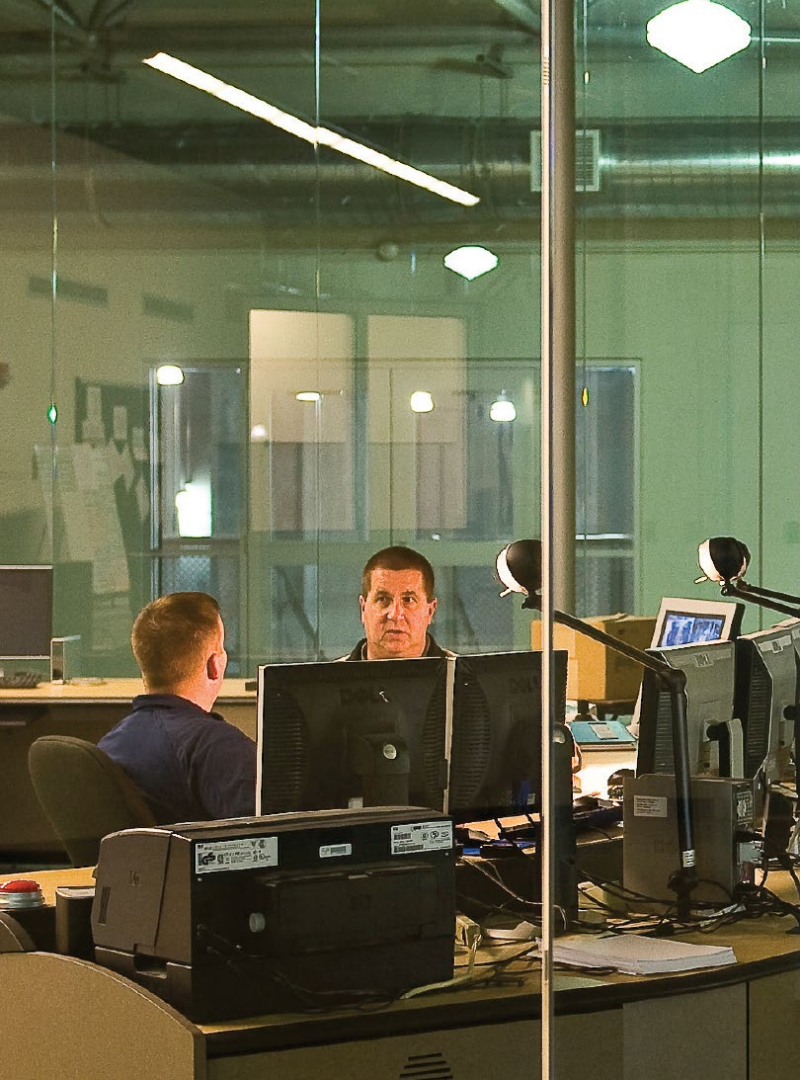
Cybersecurity UFC Design Requirements (not CMMC)

January 22, 2024

Presenter

David Brearley, GICSP. CISM, PMP
Operational Technology Cybersecurity Director
David.Brearley@hdrinc.com
Office: 704.338.6853
Cell: 732.646.3086



Agenda

01 **Identifying AE Cyber Requirements**

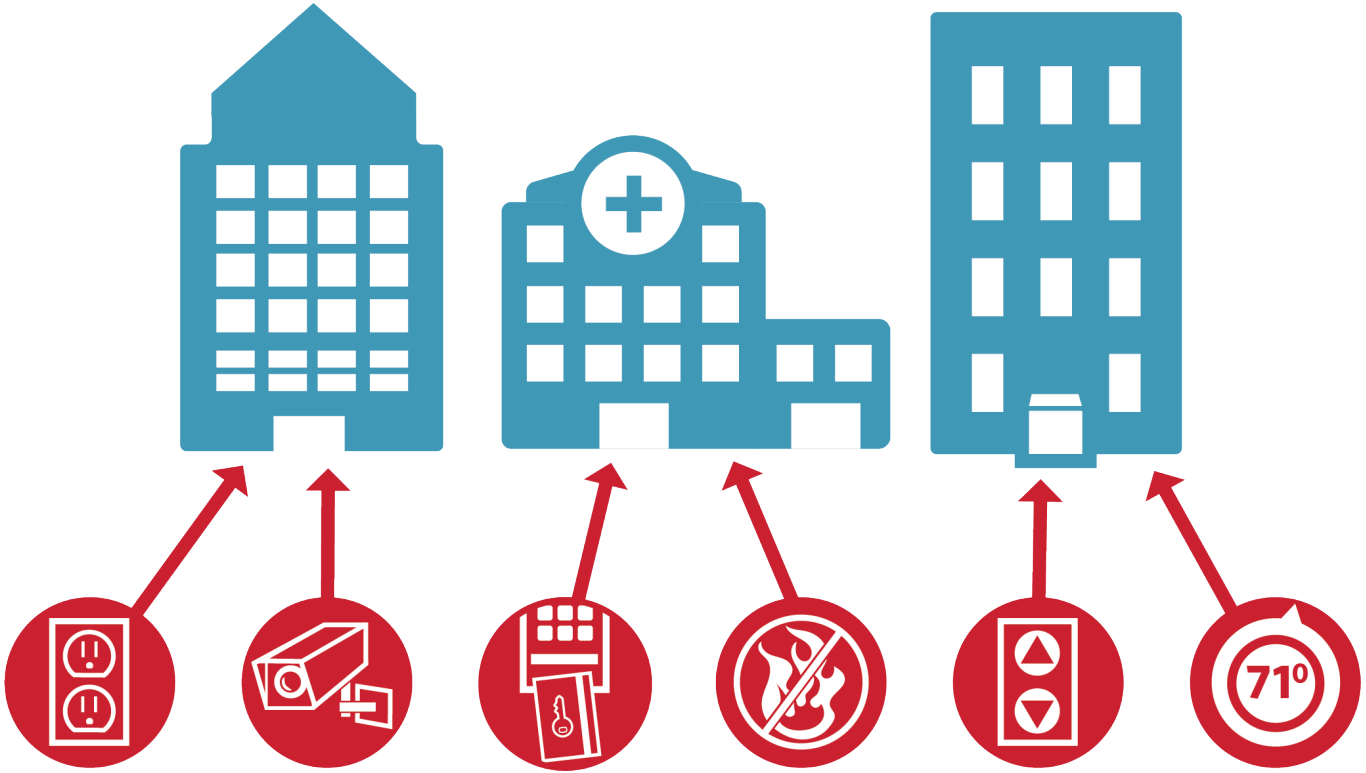
02 **What is Required of AE?**

03 **Impact on Construction**

04 **Q&A**

01 Identifying AE Requirements

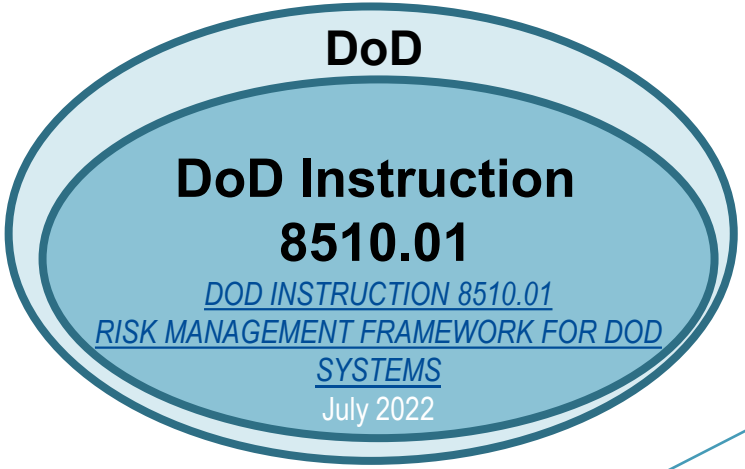
Cybersecurity Threats to Critical Infrastructure



Examples of Operational Control Systems Found in Critical Infrastructure

- HVAC/Mechanical
- Wastewater Treatment
- Water Treatment
- Oil/Water Separator
- EV Charging
- Emergency Generators
- Automated Blinds
- Photovoltaic Systems
- Occupancy Controls
- Geolocating / Tracking
- Lighting
- ESS
- Many more…

DoD Military Mandate – RMF FOR DOD SYSTEMS



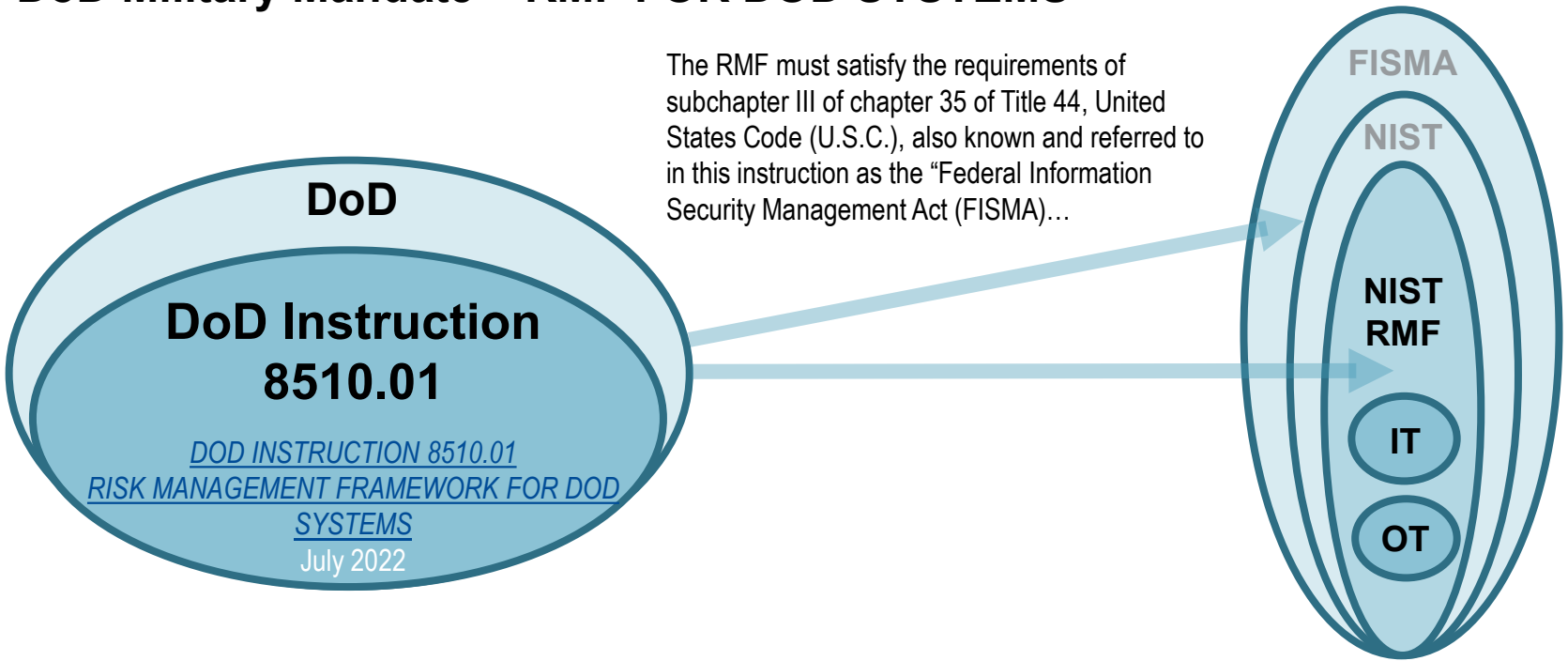
Newest 2022 version Reissues and Cancels DoD Instruction 8510.01 which was named *Risk Management Framework (RMF) for* ***DoD Information Technology (IT)*** and is now named *Risk Management Framework for* ***DoD Systems***

"The RMF process applies to all systems and organizations regardless of acquisition pathway in the DoD, as well as DoD partnered systems and organizations where it has been agreed that DoD standards will be followed." *According to* Section 3, sub-section 3.1 OVERVIEW, sub- sub-section (c) of this new release *this shall include the following systems:*

(1) **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. Refer to the RMF KS for additional guidance on authorizations.*

DoD Military Mandate – RMF FOR DOD SYSTEMS

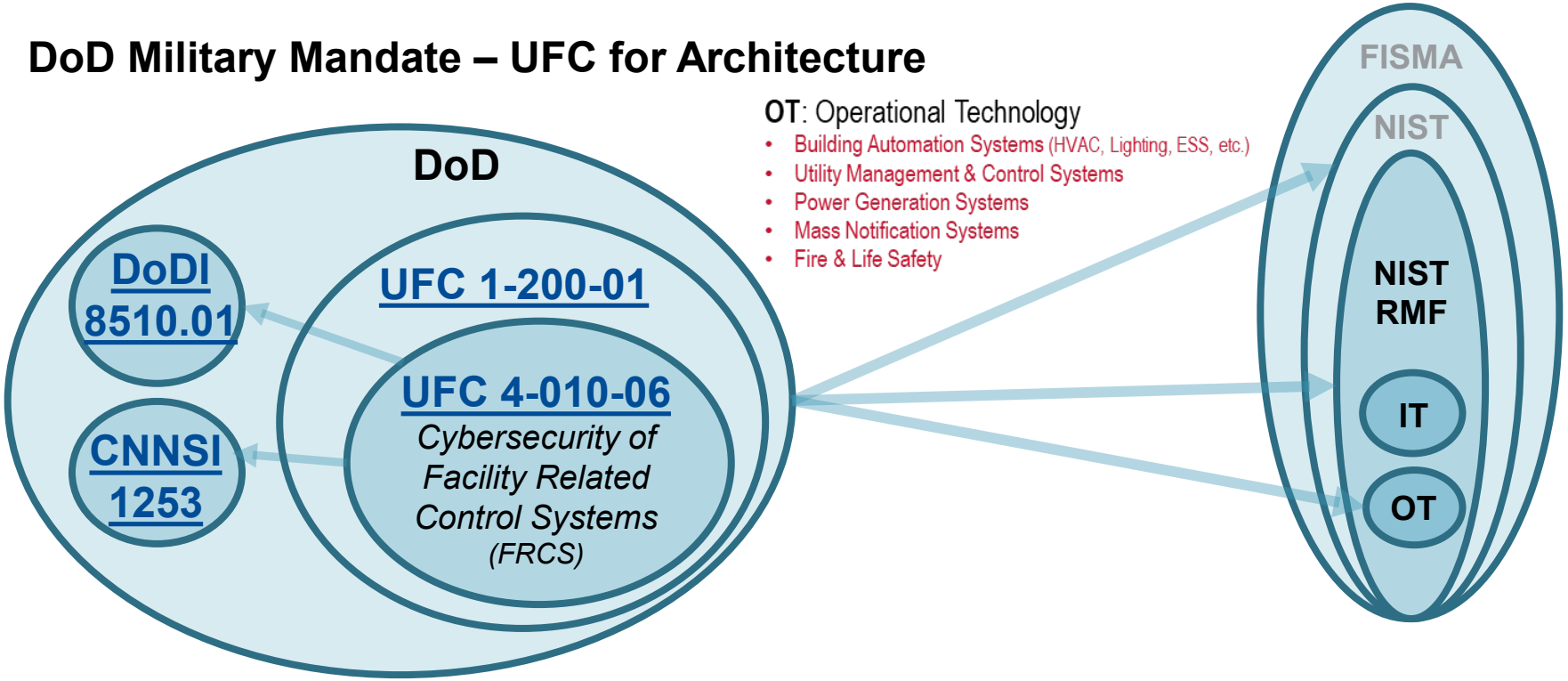
The RMF must satisfy the requirements of subchapter III of chapter 35 of Title 44, United States Code (U.S.C.), also known and referred to in this instruction as the "Federal Information Security Management Act (FISMA)…



The cybersecurity requirements for DoD information technologies will be managed through the RMF consistent with the principals established in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 (Reference (c)). DoD IS and **PIT** systems will transition to the RMF in accordance with…

PIT: Platform Informational Technology = Military OT

DoD Military Mandate – UFC for Architecture



Description: UFC 4-010-06 provides requirements for incorporating cybersecurity into the design of facility-related control systems and is a CORE UFC requirement. Per UFC 1-200-01, Section 1-6.3.1.1 Core UFC, all DoD MILCON funded project must *"Comply with the Core UFC listed here."*

The UFC 4-010-06 is a CORE UFC that provides criteria for the inclusion of cybersecurity in the design of control systems in order to address appropriate Risk Management Framework (RMF) security controls **during design and subsequent construction**.

Cybersecurity Expertise (RFPs and 25 05 11 – Qualifications)

Look Out for DoDi 8570 & 8540 – Staff Qualification Requirements

Individuals performing cybersecurity design functions shall meet certification and skills requirements for IAM Level II Certified Professional outlined in DoD 8140 Information Assurance Workforce Improvement Program. It is the Contractor's responsibility to ensure the latest DoD, Component and installations policies and guidance are met for the requirements.

Cybersecurity consultants shall attend on-site site/investigation/Charrette.

Control System Cybersecurity Subject Matter Expert

"The individual will oversee all work within this specification. This position requires that the individual currently meets Information Assurance Manager Level II Certification in accordance with DoDI 8570 Information Workforce Improvement Program.

Individuals for this position should have experience securing DoD systems and with Risk Management Framework. All certifications to include computing environment must be in effect prior to beginning work."

Computing Environment (System Administrator) and Networking Personnel

"The individual will complete all work at the computing level environment. This position requires that the individual meets Information Assurance Technical Level II Certification in accordance with DoDI 8570 Information Workforce Improvement Program.

Individuals for this positions should have experience securing DoD systems, Security Information Technical Guides, associated tools and practices. Control System Experience is highly desirable."

Additional Statement.

"Control System Cybersecurity Subject Matter Expert and Computing Environment and Network Personnel can serve across the contract"

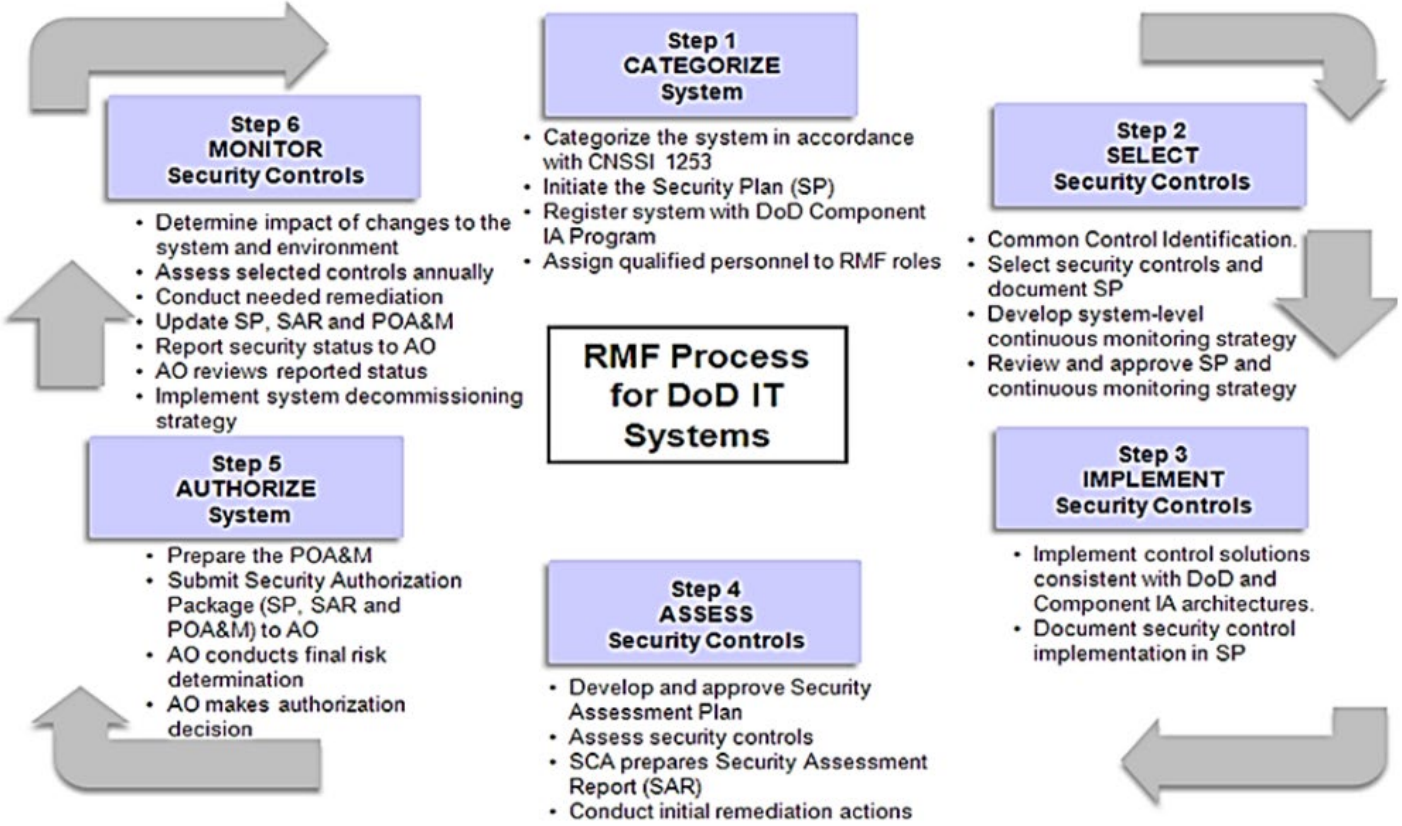
Requirements by Agency

- Department of Defense
  - UFC-4-010-06
    - Included by reference to UFC 1-200-1
  - Includes DIA, DHA, NASA, DLA
  - Applies regardless of network connectivity
  - Applies to temporary systems
- DoE Directive 205.1C
- USDA / GSA / DHS
  - Utilize NIST 800 for Agency Compliance
- VA (Design Manual – Chapter 10)
- Dams & Levees (Dams C2M2)
  - Annual Security Compliance Certification (ASCC)
  - Security Assessment Template for Group 2 Dams
  - USACE ER-25-1-113
- National Parks Service (ACIO-2020-002)
- National Institute of Health (NIH) – Design Requirements Manual
  - Reference BAS DHS Cyber Reqs
- Power / Energy – NERC/FERC

02 What is Required of AE?

Risk management framework (RMF) - Review

Figure 3. RMF process chart.



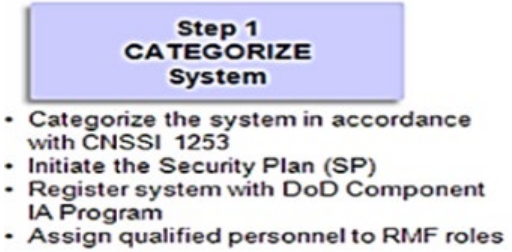
Cyber UFC Design Activities

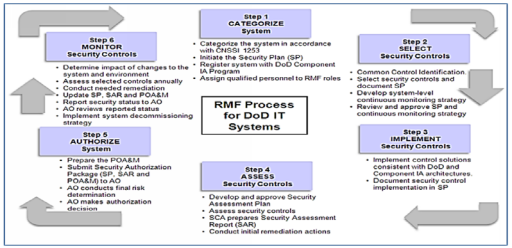
Design Bid Build Designer Steps 1-5	Basis of Design (Does not go to Contractor)	CCI List (Does not go to Contractor)	Cost Estimate (HDR Tool)	Cost Estimate (dd1391 Programmed)	Specification Table of Contents	Tailored Specification 25 05 11 per system **	Include Qualifications in 25 05 11 ***	Tailored Specification 25 08 11.00 20	Review of Related Specifications	Review of Network Diagrams
15% Design / Concept / Charrette Report (Step 1)	X			X						
35% Design and Below (Step 2 - 4 CCIs)	X	X	Internal	X	X				X	
60% Design (Step 5 - Specs / Maintain Steps 1-4)	X	X	X	X		X	Y		X	X
Pre-Final Design (~95%) (Step 5 - Specs / Maintain Steps 1-4)	X	X	X	X		X	Y		X	X
Final Design (100%) (Step 5 - Specs / Maintain Steps 1-4)	X	X	X	X		X	Y		X	X
Issued for Construction (IFC) (Step 5 - Specs / Maintain Steps 1-4)	X	X	X	X		X	Y		X	X
Conformed Package (Step 5)						X	Y		X	X

- UFC-4-010-06 Chapter 5 Designer Requirements
  - 15% / Concept
    - CIA Ratings
    - Network Connectivity
    - Authorization Plan
    - System Owners
    - Initial CCI List
  - 35%
    - Tailored CCI List
    - CONOPs
    - Network Concept Diagrams
  - 60%-Final
    - Specifications
      - UFGS 25 05 11 (Primary)
      - UFGS 25 08 10
      - UFGS 25 10 10 (jointly w/ mechanical)
      - UFGS 25 08 11.00 20 (Navy Only)
      - Coordinate security controls into all other discipline specifications
    - Drawings
      - Support Network Diagrams

Basis of Design (10-15%)

- Identify Systems
- System Descriptions
- Mission Rating (Support, Essential, or Critical)
- Determine/Verify System CIA Impact Level on the mission (L/M/H)
  - C = Confidentiality
  - I = Integrity
  - A = Availability
- Starting Security Control Set and Tailoring Recommendations
- Identify & Confirm with System Owners / Authorizing Officials
- Network Connectivity Descriptions
- System Connections





Asset Group	System	C-I-A
Life Safety	Radio and Public Address System	MMH
	Fire Detection and Alarm System	
ESS	Electronic Security Systems	MMM
Utility Monitoring & Control System - MMM	HVAC (Critical Systems)	MMH
Utility Monitoring & Control System - MML	HVAC (Standard Areas)	MML
	Electrical Systems	
	Lighting Control System	
	Uninterruptible Power Supply (UPS) System	
	Utility Monitoring and Control Systems	
Building Control System	Elevators	LLL
Monitoring Systems	Generator Monitoring and Alarm System	MMM
	Fume Hood Alarm System	
	Refrigerator Monitoring Systems	

Concept Design (30-35%)

Analysis, Documentation, and Required Client Approval

- DoD = Control Correlation Identifier (CCI List)
- One CCI List per System Group (HVAC, FLS, BAS, etc.)
- Each CCI List
  - Select CCIs from UFC based CIA Rating
  - Up To 1542 CCIs to Evaluate for each system
  - Determine Applicability and Responsibility

AH	Control Number	800-53 Control Text Indicator	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Applicable to a Cost System	DoD-Define	Enclave	Designer	Non-Designa	Impractical	Removed From Lo	N/A Justificat	REM Justificat	Combined Categor	UFGS REFERENCE
45	SC-7	SC-7(c)	CCI-001098	The information system connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.	The organization being inspected/assessed designs the information system to enforce requirements that components connect to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security	The organization conducting the inspection/assessment obtains and examines network topology diagrams, architecture documentation, or any other documentation identifying component connectivity to ensure the organization being inspected/assessed connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.	TRUE		X							Enclave	3.7.5 Process Isolation and Boundary Prot
47	SC-7(4)	SC-7(4)(a)	CCI-001102	The organization implements a managed interface for each external telecommunication service.	The organization being inspected/assessed designs the information system to have a managed interface for each telecommunication service.	The organization conducting the inspection/assessment obtains and examines network topology diagrams, architecture documentation, or any other documentation identifying system interfaces to ensure the organization being inspected/assessed implements a managed interface for each external	TRUE		X							Enclave	3.7.5 Process Isolation and Boundary Prot

Interim through Final Design (60% to Final)

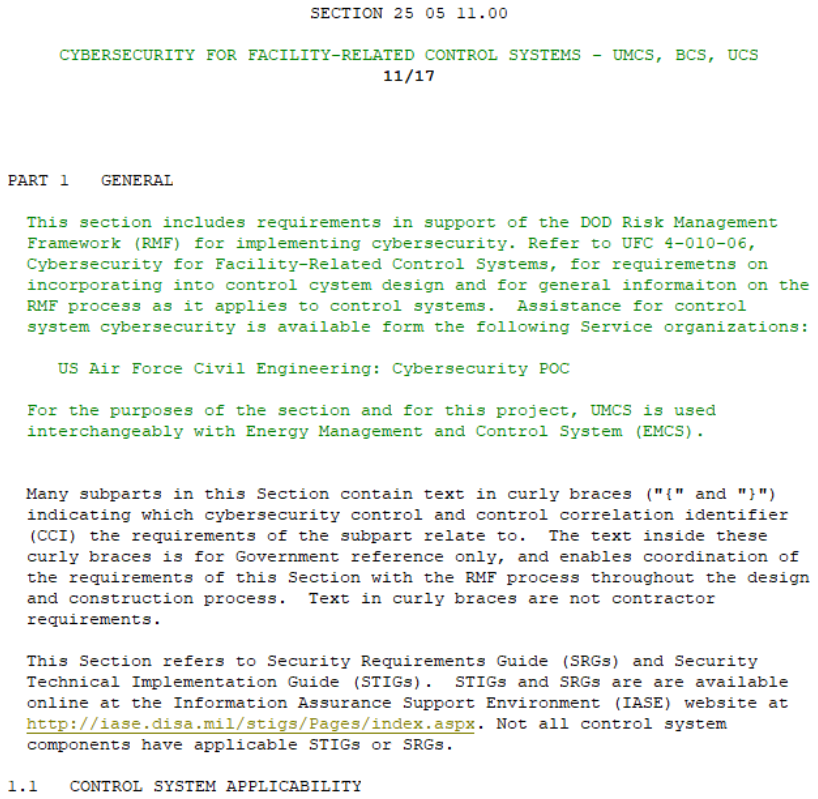
Follows normal design progression UFGS:

- 25 05 11 (one per system)
- 25 08 10 (one per system)
- 25 10 10 (one per front-end)
- 25 08 11.00 20 (NAVY Only)

Redline (e.g., *"Design"*) the Specifications based on approved & *"Tailored"* CCI list by (See Chapter 5 of 4-010-06 and Previous Slide):

1. Incorporated that CCI into the control system design by including it into these specifications where needed
2. Document any changes from standard CCI requirements, or selections made when multiple options are available.

Discipline specific coordination through 100% Issuance



SECTION 25 05 11.00

CYBERSECURITY FOR FACILITY-RELATED CONTROL SYSTEMS - UMCS, BCS, UCS
11/17

PART 1 GENERAL

This section includes requirements in support of the DOD Risk Management Framework (RMF) for implementing cybersecurity. Refer to UFC 4-010-06, Cybersecurity for Facility-Related Control Systems, for requiremetns on incorporating into control system design and for general informaiton on the RMF process as it applies to control systems. Assistance for control system cybersecurity is available form the following Service organizations:

US Air Force Civil Engineering: Cybersecurity POC

For the purposes of the section and for this project, UMCS is used interchangeably with Energy Management and Control System (EMCS).

Many subparts in this Section contain text in curly braces ("{" and "}") indicating which cybersecurity control and control correlation identifier (CCI) the requirements of the subpart relate to. The text inside these curly braces is for Government reference only, and enables coordination of the requirements of this Section with the RMF process throughout the design and construction process. Text in curly braces are not contractor requirements.

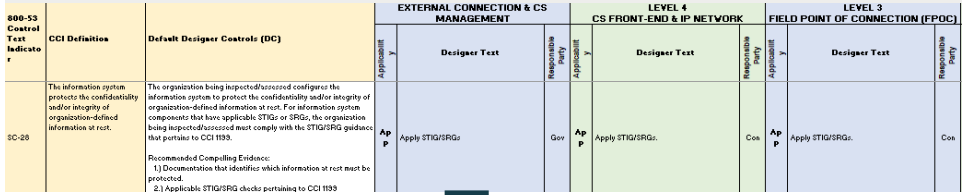
This Section refers to Security Requirements Guide (SRGs) and Security Technical Implementation Guide (STIGs). STIGs and SRGs are are available online at the Information Assurance Support Environment (IASE) website at http://iase.disa.mil/stigs/Pages/index.aspx. Not all control system components have applicable STIGs or SRGs.

1.1 CONTROL SYSTEM APPLICABILITY

Cyber UFC Design Activities

Asset Group	System	C-I-A
Life Safety	Radio and Public Address System	MMH
	Fire Detection and Alarm System	
ESS	Electronic Security Systems	MMM
Utility Monitoring & Control System - MMM	HVAC (Critical Systems)	MMH
Utility Monitoring & Control System - MML	HVAC (Standard Areas)	MML
	Electrical Systems	
	Lighting Control System	
	Uninterruptible Power Supply (UPS) System	
	Utility Monitoring and Control Systems	
Building Control System	Elevators	LLL
Monitoring Systems	Generator Monitoring and Alarm System	MMM
	Fume Hood Alarm System	
	Refrigerator Monitoring Systems	

CCIs Selected Based Upon CIA Rating (200-300+ Reponses)



800-53 Control Text Indicator	CCI Definition	Default Designer Controls (DC)	EXTERNAL CONNECTION & CS MANAGEMENT			LEVEL 4 CS FRONT-END & IP NETWORK			LEVEL 3 FIELD POINT OF CONNECTION (FPOC)		
			Applicability	Designer Text	Responsible Party	Applicability	Designer Text	Responsible Party	Applicability	Designer Text	Responsible Party
SC-28	The information system protects the confidentiality and/or integrity of organization-defined information at rest.	The organization being inspected/assessed configures the information system to protect the confidentiality and/or integrity of organization-defined information at rest. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1199. Recommended Compelling Evidence: 1.) Documentation that identifies which information at rest must be protected. 2.) Applicable STIG/SRG checks pertaining to CCI 1199	App	Apply STIG/SRGs	Gov	App	Apply STIG/SRGs.	Con	App	Apply STIG/SRGs.	Con

Follows normal design progression UFGS:

- 25 05 11 (one per system)
- 25 08 10 (one per system)
- 25 10 10 (one per front-end)
- 25 08 11.00 20 (NAVY Only)

Redline (e.g., *"Design"*) the Specifications based on approved & *"Tailored"* CCI list by (See Chapter 5 of 4-010-06 and Previous Slide):

1. Incorporated that CCI into the control system design by including it into these specifications where needed
2. Document any changes from standard CCI requirements, or selections made when multiple options are available.

Discipline specific coordination through 100% Issuance

```
{For Government Reference Only:  This subpart (and its subparts) relates to
CA-9, PL-8; CCI-002102, CCI-002103, CCI-002104, CCI-002105, CCI-003072,
CCI-003073, CCI-003075 and also the submittal requirements associated with
CM-6, CM-7, SC-8 and SC-41 including CM-7(3), CCI-000388.}
```

Interim through Final Design (60% to Final) – October 10 2023 Impacts

- Impact on Cyber Discipline
  - Each FRCS System:
    - CCI List Required at 15%
    - CCI List Overlays
    - CCI List Includes Non-Design and Enclave (1542 rows)
    - New UFGS to be Released in December
  - Detailed Interdisciplinary and Gov't Coordination Expectations
  - FRCS Grouping by Mission Served

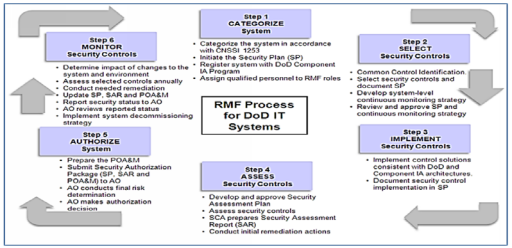
- Impact on Other Disciplines
  - Each FRCS System:
    - Network Drawings Required
    - Mission Space Drawing Required
    - Physical Security Review and Coordination
  - Moderate Rated Systems – Additional Control System Design Complexities
  - Systems Interconnected with Mixed Ratings (i.e. LLL HVAC interfacing with MMM HVAC for server room) – additional design requirements

03 Impact on Construction

Implement Security Controls (Contractor)

Each FRCS Supplier follows Div. 25 Specifications to:

- Provide documentation for DoD review and entry into eMASS
  - Detailed Network Diagrams (Physical and Logical)
  - Ports and Protocol Information
  - Security Plans
  - Product configuration
- Install & Configure FRCS devices (per security controls list)
- Coordinate with government (passwords, IP, user roles/privileges, etc)
- Security Assessment Plan
- Apply STIGs/SRGs
- Cyber Training

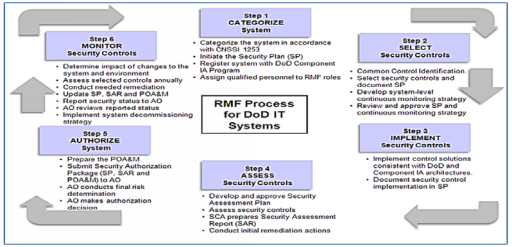


Assess Security Controls – Contractor or Government

- Security Assessment Report
- Cyber Testing
- Cyber Performance Verification Tests (PVTs)
- Remediate deficiencies
- Independent verification of configuration
- US Government audit of cybersecurity work completed
  - NAVY: Independent Contractor per 25 08 11.00 20

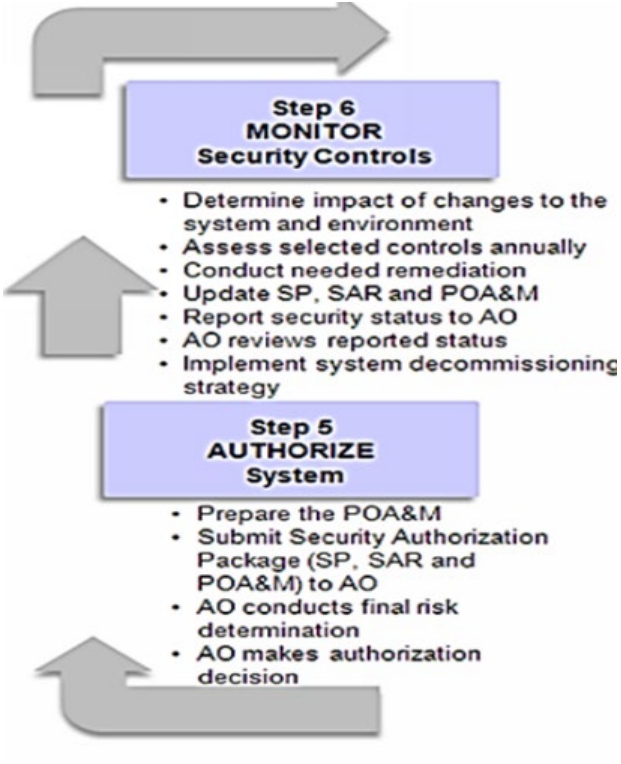
Step 4
ASSESS
Security Controls

- Develop and approve Security Assessment Plan
- Assess security controls
- SCA prepares Security Assessment Report (SAR)
- Conduct initial remediation actions



Authorize System & Monitor – Not Construction or Design

- Step 5 - Authorize
  - Each FRCS System:
    - Government System Owner or Authorizing Official reviews all work completed and eMass
    - Grant Authority to Operate (acceptance of properly configured system)
- Step 6 - Monitor
  - Facility owner must monitor system including maintenance of system to maintain security posture



04 Q&A