Cybersecurity- NAVFAC & USACE

Moderator: Col. Brian May, USAF (Ret.), Michael Baker Int'l

Speakers:

- David Gary, P.E., NAVFAC Atlantic
- Tim Nauman, Electrical Engineer, USACE Europe District

Cybersecurity- NAVFAC

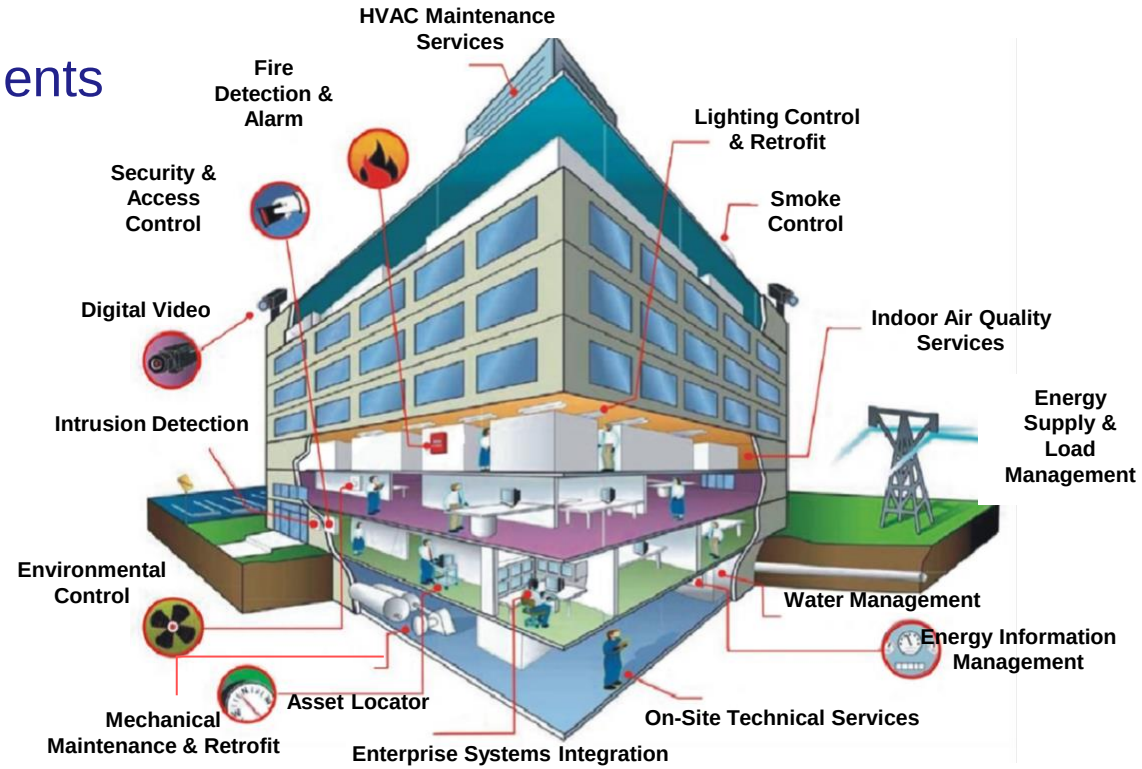
Orientation

- **Facility Related Control Systems (FRCS) Cybersecurity**
  - **CYBERSECURITY IS A CORE NAVFAC FUNCTION AND RESPONSIBILITY**
  - **All FRCS require Cybersecurity Commissioning.**
  - **NAVFAC is the Functional Authorizing Official for shore-based control systems or FRCS**
- **Cybersecurity Commissioning (CyCx)**
  - **CyCx is the execution of Cybersecurity in planning, design, and construction of facility projects**
  - **If a project includes a digital/IT system, Cybersecurity is a requirement, not an option.**
  - **UFC 4-010-06 “Cybersecurity of Facility-Related Control Systems” is a Core UFC.**
  - **CyCx satisfies a percentage of controls in an authorization effort.**

NAVFAC Naval Facilities Engineering Systems Command

Authorities

- **Technical Authority for Facilities IT: *(SECNAVINST 5400.15, OPNAVINST 5239.1)***
  - Responsible for technical and engineering conformity to Navy cybersecurity standards
- **Functional Security Control Assessor**
  - Responsible for cybersecurity risk assessments
- **Authorizing Official**
  - Responsible for the authorization and cybersecurity oversight:
    - Transportation
    - Weight handling equipment
    - Anti-terrorism/force protection ashore
    - Facility and Utility control systems
    - Contingency engineering
    - Expeditionary



Situation

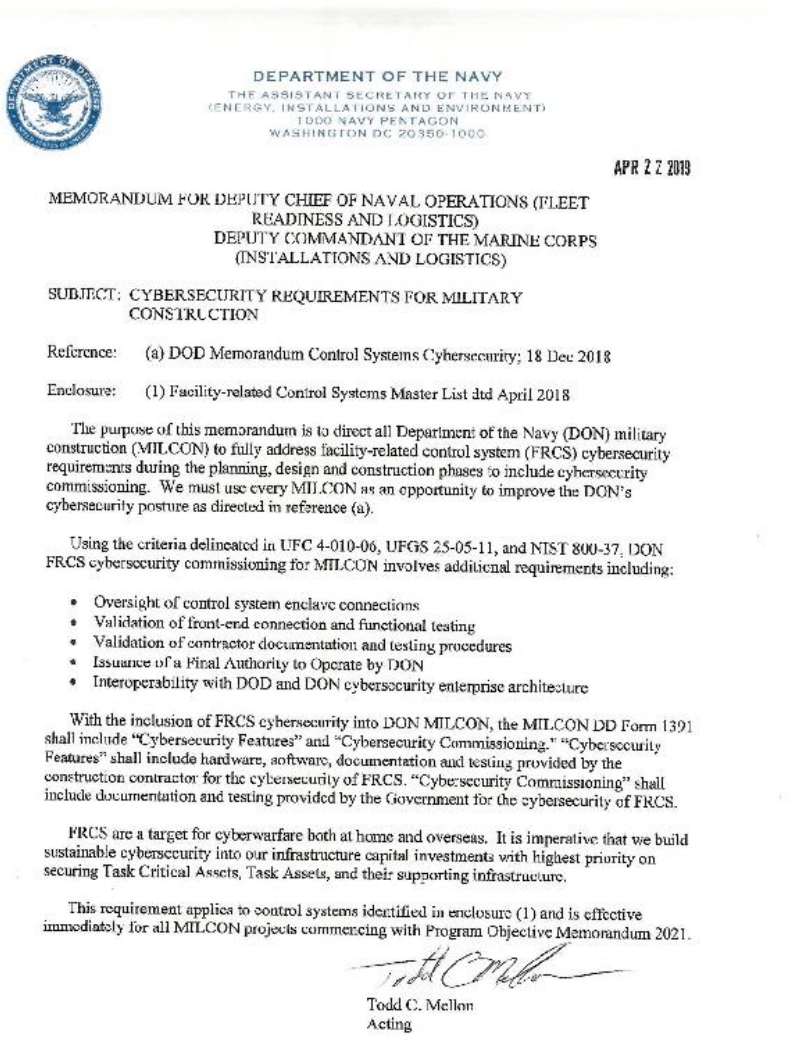
- In 2018 SECNAV memo defined Cybersecurity Commissioning and Cybersecurity Features for Navy and Marine Corps Military Construction to begin in FY21.

- CyCx was established for cybersecurity support in the execution of Risk Management Framework (RMF) packages and requirements in the Unified Facility Guide Specifications (UFGS) 25 05 11 Cybersecurity for FRCS.

- The purpose is to embed cybersecurity requirements into the Design & Construction process to deliver construction projects that meet all cybersecurity requirements prior to occupancy.

NAVFAC Naval Facilities Engineering Systems Command

SECNAV MEMO



DEPARTMENT OF THE NAVY
THE ASSISTANT SECRETARY OF THE NAVY
(ENERGY, INSTALLATIONS AND ENVIRONMENT)
1000 NAVY PENTAGON
WASHINGTON DC 20350-1000

APR 2 2 2019

MEMORANDUM FOR DEPUTY CHIEF OF NAVAL OPERATIONS (FLEET READINESS AND LOGISTICS)
DEPUTY COMMANDANT OF THE MARINE CORPS (INSTALLATIONS AND LOGISTICS)

SUBJECT: CYBERSECURITY REQUIREMENTS FOR MILITARY CONSTRUCTION

Reference: (a) DOD Memorandum Control Systems Cybersecurity; 18 Dec 2018

Enclosure: (1) Facility-related Control Systems Master List dtd April 2018

The purpose of this memorandum is to direct all Department of the Navy (DON) military construction (MILCON) to fully address facility-related control system (FRCS) cybersecurity requirements during the planning, design and construction phases to include cybersecurity commissioning. We must use every MILCON as an opportunity to improve the DON's cybersecurity posture as directed in reference (a).

Using the criteria delineated in UFC 4-010-06, UFGS 25-05-11, and NIST 800-37, DON FRCS cybersecurity commissioning for MILCON involves additional requirements including:

- Oversight of control system enclave connections
- Validation of front-end connection and functional testing
- Validation of contractor documentation and testing procedures
- Issuance of a Final Authority to Operate by DON
- Interoperability with DOD and DON cybersecurity enterprise architecture

With the inclusion of FRCS cybersecurity into DON MILCON, the MILCON DD Form 1391 shall include "Cybersecurity Features" and "Cybersecurity Commissioning." "Cybersecurity Features" shall include hardware, software, documentation and testing provided by the construction contractor for the cybersecurity of FRCS. "Cybersecurity Commissioning" shall include documentation and testing provided by the Government for the cybersecurity of FRCS.

FRCS are a target for cyberwarfare both at home and overseas. It is imperative that we build sustainable cybersecurity into our infrastructure capital investments with highest priority on securing Task Critical Assets, Task Assets, and their supporting infrastructure.

This requirement applies to control systems identified in enclosure (1) and is effective immediately for all MILCON projects commencing with Program Objective Memorandum 2021.

Todd C. Mellon
Acting

CyCx Mission

Mission:
NAVFAC will deliver cybersecurity assessed systems at beneficial occupancy in support of Maximizing Shore Readiness and Securing Mission Relevant Cyber Terrain.

End State:
Facility systems acquired in conjunction with construction will be delivered in an assessed and authorized state.

NAVFAC Naval Facilities Engineering Systems Command

Risk Management Framework Steps

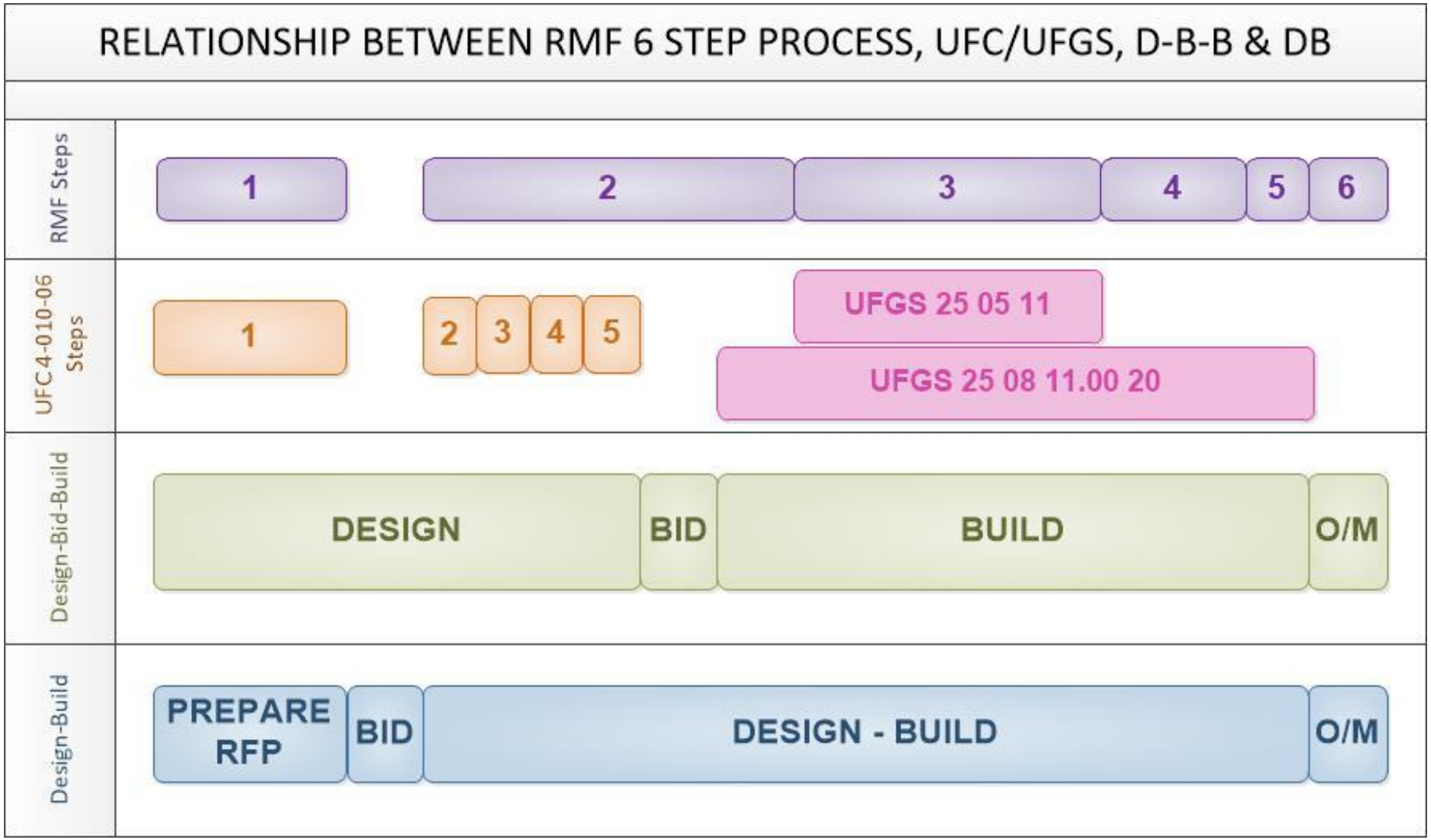
1. Categorize System
2. Select Controls
3. Implement Controls
4. Assess Controls
5. Authorize System
6. Continuous Monitoring

CyCx Process

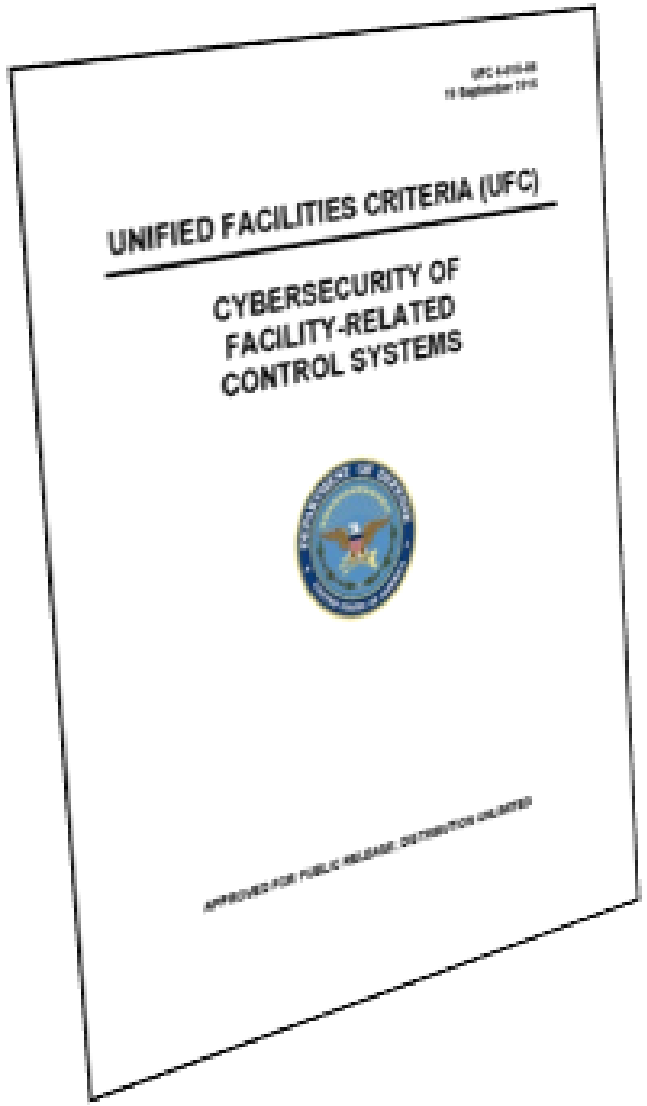
- Cybersecurity Commissioning begins in the planning phase and continues beyond facility acceptance.
- Risk Management Framework is done in parallel with construction providing assessed and authorized systems in conjunction with beneficial occupancy.
- This commissioning process adds Cybersecurity requirements as applicable through an evaluation of information types and system criticality.
- The Unified Facility Criteria (UFC 4-010-06) aligns contractor Risk Management Framework responsibility to the design and construction process.
- The Unified Facility Guide Specification (UFGS 25 05 11) is construction contract language edited to satisfy a portion of the Cybersecurity requirements in construction.

NAVFAC Naval Facilities Engineering Systems Command

Process Alignment

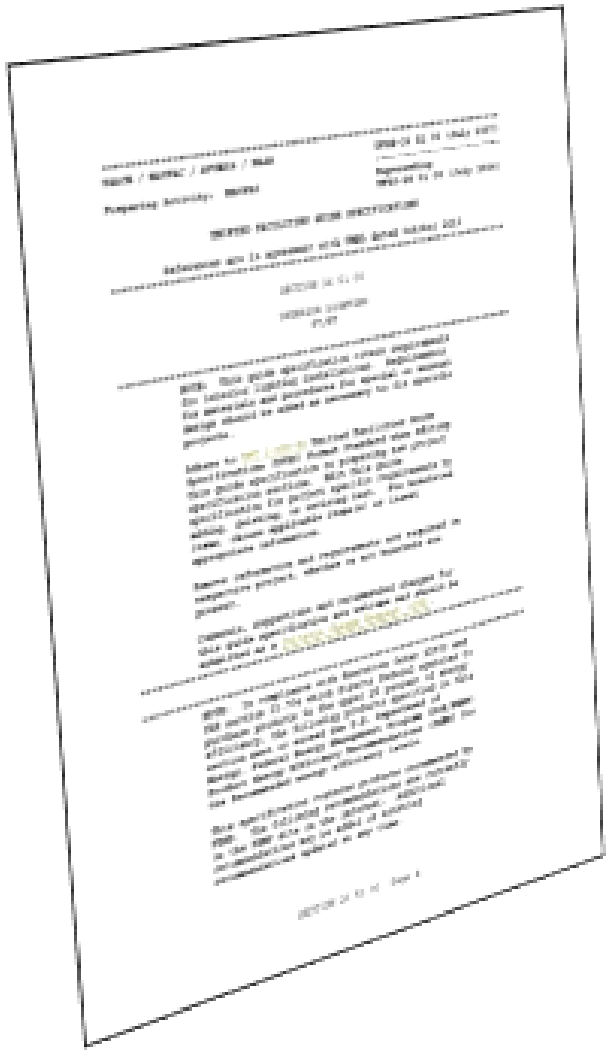


UFC 4-010-06 CYBERSECURITY OF FACILITY-RELATED CONTROL SYSTEMS



- Integrates Risk Management Framework (RMF) design and construction requirements for facility-related control systems.
- Applies to all new construction and repair projects
- Guidance to Designers-of-Record
- Details provided for LOW and MODERATE impact systems
- HIGH impact systems require special attention (IAT II/Security+ Professional)

UFGS 25 05 11 CYBERSECURITY OF FACILITY-RELATED CONTROL SYSTEMS



- Implements cybersecurity into construction projects for facility-related control systems
- Contains construction contract language edited to satisfy contractor responsible Cybersecurity requirements.
- Includes construction submittals which support RMF
- Covers LOW and MODERATE Impact Systems and aligns with requirements for assess only.

UFGS 25 08 11.00 20 RMF OF FACILITY-RELATED CONTROL SYSTEMS

- The UFGS 25 08 11.00 20 adds a cybersecurity security professional to the contractor team
- Provides translation of submittals into RMF artifacts
- Requires the contractor to have eMASS access and execute work inside eMASS.
- The government provides the contractor with a CAC card for eMASS access.
- UFGS 25 08 11.00 20 is used in conjunction with UFGS 25 05 11 to enhance the cybersecurity requirements of the contractor.
- Can be added to projects requiring eMASS support such as Assess Only Package and Authority to Operate

Standardization

- NAVFAC is pursuing facility-related control system standardization by:
  - Control system function
  - And installation or geographic area

- The standardization process includes:
  - Business case analysis
  - Class Justification and Approval (CJ&A)
  - Authorization
  - Standard Specifications

- Reducing disparity and control systems across the enterprise is critical to our sustainment and cybersecurity strategy.

- Standardization is governed by NAVFAC instruction 11000.2

CyCx Toolbox Overview

- Tailored Specifications and Change Request / MFR
  - Install something from existing Authorization, J&A/CJ&A
- UFC 4-010-06 + UFGS 25 05 11 + Change Request / MFR
  - Full and Open Design, but CTR submits for Component w/ Auth
- UFGS 25 08 11
  - Enhancement to UFGS 25 05 11 with eMASS & RMF Artifacts
- UFC 4-010-06 + UFGS 25 05 11 + ATO
  - Commissioning with ATO in Parallel
- UFC 4-010-06 + UFGS 25 05 11
  - Simple Commissioning, “Authorizable” System
- Cyber Hygiene Checklist
  - Low-Cost Checklist pre-2017, Pre-UFC 4-010-06
- Do nothing at all (No FRCS)

NAVFAC Naval Facilities Engineering Systems Command

Cybersecurity-USACE

CYBERSECURITY DESIGN FOR USACE PROJECTS IN EUROPE

Tri-Services Government Industry Engagement
Naples, Italy
28 February 2024

Tim Nauman, Electrical Engineer
USACE Europe District
CENAU-ECE
timothy.j.nauman@usace.army.mil

U.S. ARMY

US Army Corps of Engineers®

TODAY'S TAKEAWAYS

- Cybersecurity – this is what it means to us
- What we get for our money
- Making use of what we are buying

CYBERSECURITY

Protects

- Computers
- Control Systems
- Network Services and
- Data

From

- Damage
- Theft
- Disruption
- Misdirection

By these guys…

DOD PROJECT CYBERSECURITY

- **Unified Facility Criteria 4-010-06, Cybersecurity of FRCS**
  - **basic compliance with NIST Risk Management Framework (RMF)**
  - **to assess and manage organizational risk**

- **Describes general safeguards**
  - **based on potential impact of compromise to**
    - Confidentiality (disclosed to authorized individuals)
    - Integrity (information is accurate)
    - Availability (information available whenever needed)
- **Provides documentation about the control system**
  - **Devices**
  - **Configuration**
  - **Interconnections**

- **Very Different from**

Offensive Cyber (Service Branch Cyber Ops)

Cyber Weapons Systems
Security Operations Centers
Penetration Testing, Remote Monitoring and Access
Supply chain compromise

Defensive Cyber (DHS Critical Infrastructure)

Incident Response
Network Management
Continuous monitoring

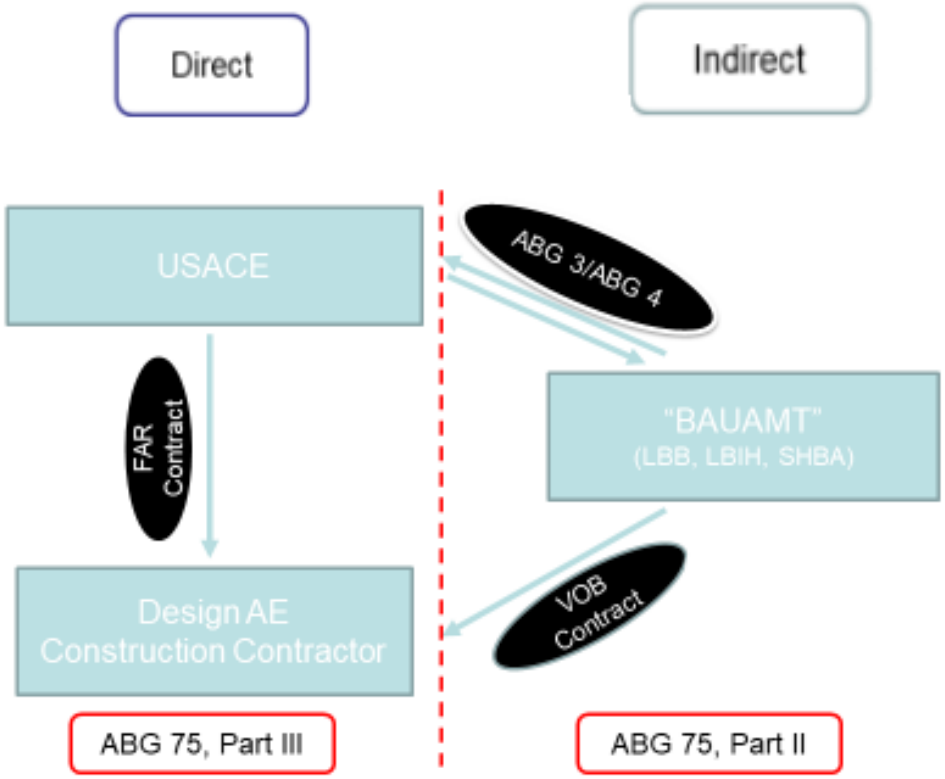
REQUIREMENTS

- **UFC 4-010-06, CYBERSECURITY OF FACILITY RELATED CONTROL SYSTEMS**
  - Implements (NIST) Risk Management Framework as policy
  - Assumes customer participation & RMF program support
  - Describes computer-based security features and documentation
  - LOW and MODERATE loss impact levels
  - Applicable Control Systems
    - Building Automation/Management
    - HVAC DDC
    - Utility/Energy Monitoring
    - Lighting Control
    - Electrical Distribution
    - Emergency Power Generation
    - Fire Alarm/Life Safety
    - Elevator Controls
    - Electronic Security Systems (IDS, Access Control, CCTV)
- **UFGS SECTION 25 05 11, CYBERSECURITY FOR FACILITY-RELATED CONTROL SYSTEMS**
  - US-based specification to satisfy the UFC
  - Actions and deliverables to construct a secure control system
  - Tailored for each control system design (HVAC,FALS,ESS)
- **Suitable for use on European projects <u>except</u> Indirect* projects in Germany**
  (Indirect projects are those awarded to the German government for execution)

UFGS DELIVERABLES

- **AE Designs the Cybersecurity Requirements using the Unified Facilities Criteria (UFC) and Unified Facilities Guide Specifications (UFGS)**
- **Contractor executes the design and delivers artifacts according to the specification**
- **Customer uses the artifacts to complete their Risk Management Framework (RMF) accreditation process**
- **Artifacts**
  - System Description
  - Network Diagram
  - Dataflow Diagram
  - Hardware and Software Lists
  - Ports, Protocols, and Services List
  - All applicable STIG Checklists with comments
  - POA&M or deviations document listing and justifying any exceptions to required patches, IAVAs, and STIGs
  - Validation test results for system construction and hardening
    - +System pre- and post security scans [NESSUS and SCAP/SCC]
- **Required for each FRCS in the project**

USACE DIRECT VERSUS INDIRECT CONTRACTS



- Auftragsbauten Grundsätze / Principles of Construction Contracting 1975 (ABG 1975)
- Vertragsordnung für Bauleistungen (VOB) / Contract Regulations for the Provision of Construction Services
- Bauamt – State Construction Authority

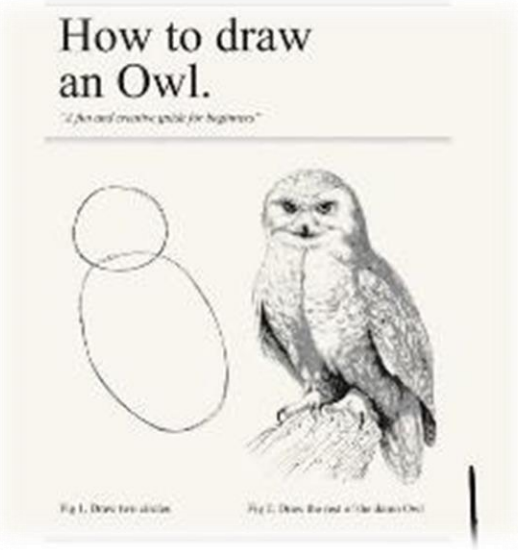
- **USACE ENGINEERING GUIDELINE 02-2021 Cybersecurity Indirect Rev 1 provides the Functional Requirements for use on Indirect Projects in Germany**

PERSPECTIVES

DESIGNER

INFO SECURITY PEOPLE

CUSTOMER'S EXPERIENCE



WHAT'S NEEDED

- **CUSTOMER**
  - Participate by identifying POCs
  - Understand what you have
    - Base-wide systems you own
    - Basics of RMF
    - How to use the artifacts in RMF
  - Recognize
    - This is facilities-related and not IT
    - You are paying for this
    - You are not expected to be the expert

- **DESIGNER**
  - Understand
    - This is a design, not a referral to standards
    - It applies to the control systems in your design
    - Research is needed for the connection to base-wide systems
  - Recognize
    - You are responsible for the design
    - The topic is not part of traditional engineering
    - The UFC and UFGS is not a how-to guide
      - CCI's are not actions or requirements
    - You are expected to be the expert

GENERAL CONCLUSIONS

- **RMF IS DIFFERENT FROM IT-BASED CYBERSECUITY**

IT'S THIS

NOT

- **EXPLANATIONS AND DESIGNS SHOULD BE UNDERSTANDABLE**
- **FINDING AN EXPERT CAN BE DIFFICULT BUT NOT IMPOSSIBLE**
- **IT'S EASY TO OVERTHINK WHAT IS NEEDED**

QUESTIONS

QUESTIONS & FEEDBACK

BACKUP

BASIC CONTROL SYSTEM COMPONENTS

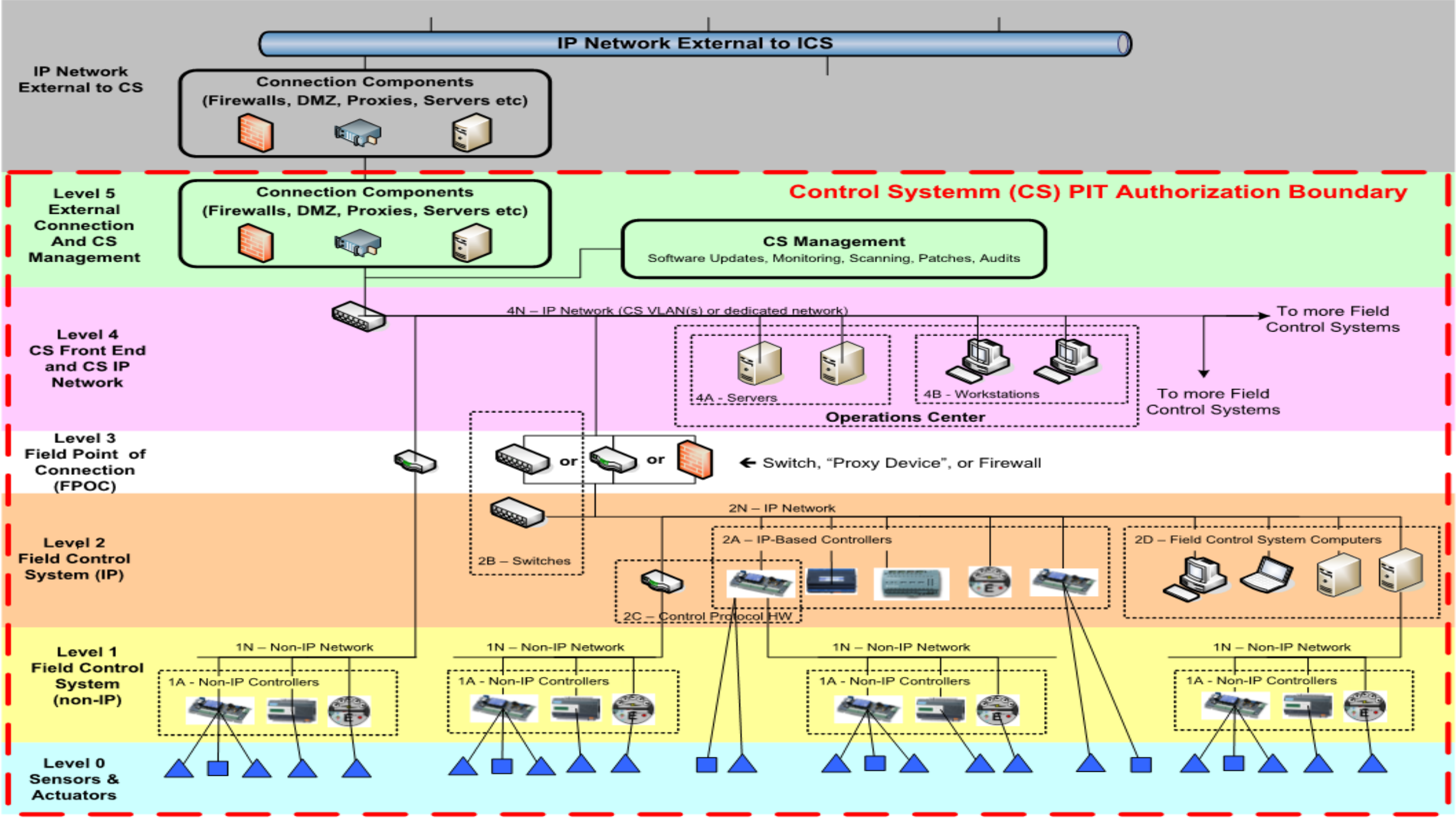
- **Controlled Equipment**: Facility equipment (e.g., T&D circuit breaker, transformer, isolation switch, etc.) that is monitored or controlled by a Control System

- **Controller**: An electronic device – usually having internal programming logic and digital & analog input/output capability – which performs control functions. Two primary types of controller are equipment controller and supervisory controller

- **Network**: Those components of the control system that are standard IT components and can be secured in a standard manner independent of the type of control system. These components serve only the control system and include the IP network, network management and security devices (e.g., switches, routers), software, computers and/or other devices which provide management and security of the network.

- **Front End**: The portion of the control system consisting primarily of IT equipment, such as computers and related equipment, intended to perform operational functions and run monitoring and control/engineering tool application software. The front end does not directly control physical systems; it interacts with them only through field control systems (FCS)

- *Most definitions from UFC 4-010-06


IP Network External to ICS
IP Network External to CS
Connection Components (Firewalls, DMZ, Proxies, Servers etc)
Control Systemm (CS) PIT Authorization Boundary
Level 5 External Connection And CS Management
Connection Components (Firewalls, DMZ, Proxies, Servers etc)
CS Management
Software Updates, Monitoring, Scanning, Patches, Audits
Level 4 CS Front End and CS IP Network
4N – IP Network (CS VLAN(s) or dedicated network)
To more Field Control Systems
4A - Servers
4B - Workstations
Operations Center
To more Field Control Systems
Level 3 Field Point of Connection (FPOC)
or
or
Switch, "Proxy Device", or Firewall
Level 2 Field Control System (IP)
2N – IP Network
2A – IP-Based Controllers
2D – Field Control System Computers
2B – Switches
2C – Control Protocol HW
Level 1 Field Control System (non-IP)
1N – Non-IP Network
1A - Non-IP Controllers
1N – Non-IP Network
1A - Non-IP Controllers
1N – Non-IP Network
1A - Non-IP Controllers
1N – Non-IP Network
1A - Non-IP Controllers
Level 0 Sensors & Actuators

RISK MANAGEMENT FRAMEWORK (RMF)

A business management strategy applied to information systems

Applies risk management activities to information systems in the system development life cycle.

Identifies risk to the organization's operation from these information systems and the mitigations needed to reduce risk to an acceptable level authorized by the organization.

Requires collaboration between organizational stakeholders in assessing and managing risks to their organization.

WHY IS THIS IMPORTANT

RMF applies to all DoD IT that receives, processes, stores, displays, or transmits DoD information.

Customer Systems must follow the RMF process for Authorization to Operate

Control System Connectivity to Base Systems can influence functionality and Authorization