Built-In Security:
Cyber-Informed Design for DoD Facilities

SAME Jacksonville Post Luncheon
September 2025

complex world | CLEAR SOLUTIONS™

Introductions

Elizabeth (Beth) Griffith, P.E., *Vice President Air Force & Space Force Programs* –

Formerly AFCEC Design & Construction Execution Technical Program Manager, Ms. Griffith joined Tetra Tech in 2023 to manage Tetra Tech's portfolio of Air Force projects. In her role at AFCEC, Ms. Griffith served as the subject matter specialist (SMS) for Cybersecurity for Facility Related Controls and implementation of UFC 4-010-06 across AFCEC's nearly $3B annual portfolio of projects. Since it's inception in 2015, Ms. Griffith has implemented execution agency, installation customers, design A-E team, and construction contractor controls to ensure Cybersecurity is comprehensively managed at each stage of a project.

OBJECTIVES

- Glossary of Relevant Terms
- RMF Process and How the UFC Fits
- Cybersecurity in Facility Design and Construction
- UFC 4-010-01 Process
- Advancements in Cybersecurity

Glossary

CYBER PHYSICAL SYSTEMS (CPS)

TETRA TECH

Mason&Hanger
A Day & Zimmerman Company

Computational elements with physical components, sensors or actuators, to monitor and control physical systems

Derived from definitions in the IOT Cybersecurity Improvement Act of 202 and NIST SP 800-37r2

OPERATIONAL TECHNOLOGY (OT)

TETRA TECH

Mason&Hanger
A Day & Zimmerman Company

Hardware and software that detect or causes a kinetic outcome through the direct monitoring or control of physical devise, processes, and events; Separate from Information Technology (IT) which manage and delivers information

Derived from definitions in the IOT Cybersecurity Improvement Act of 202 and NIST SP 800-37r2

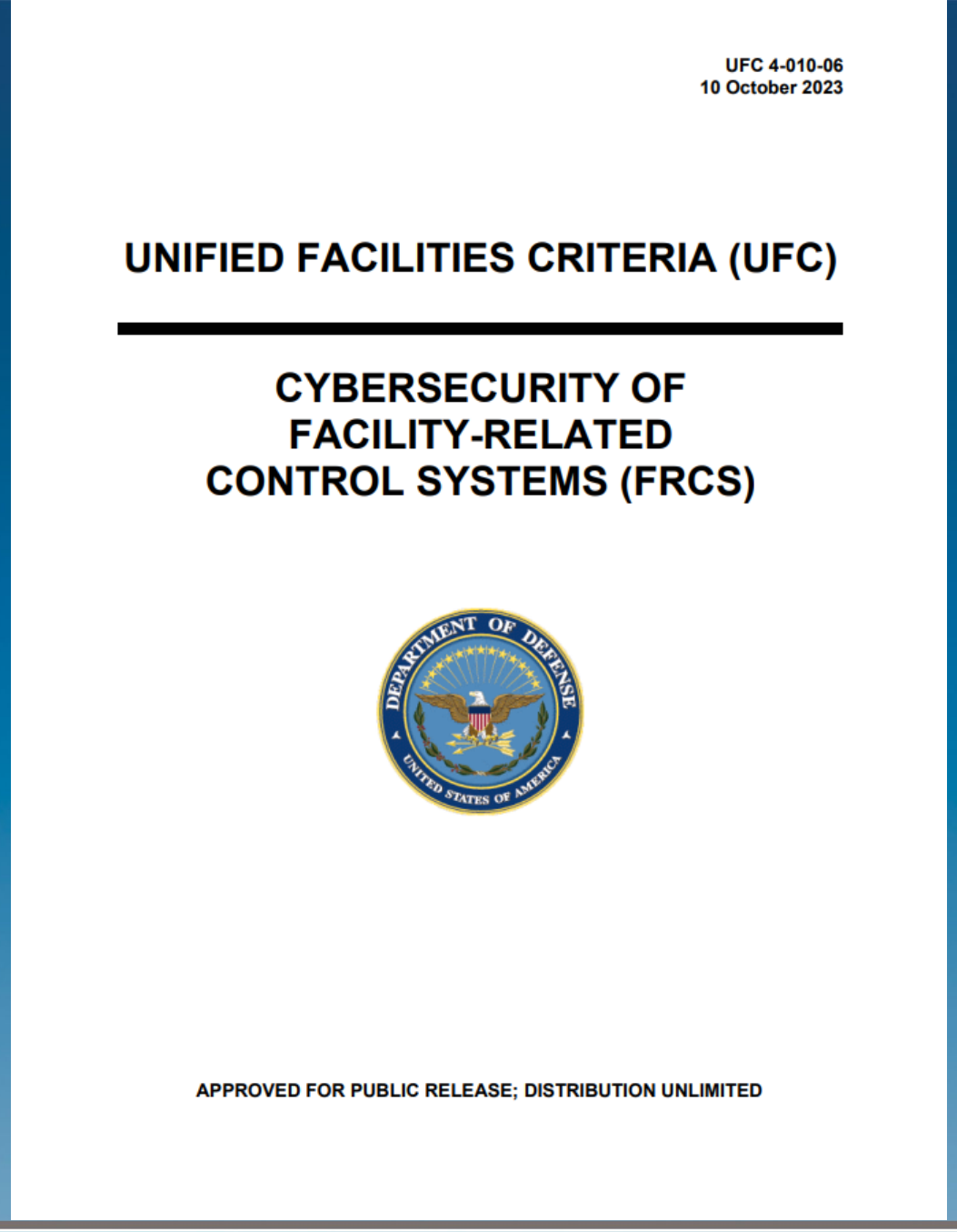
RISK MANAGEMENT FRAMEWORK (RMF)

TETRA TECH

Mason&Hanger
A Day & Zimmermann Company

A federal process documented in NIST SP 800-53, adopted to manage risk to help secure systems, controlling selection and specification of systems, assessing security, and authorizing the system for use, authorizing Authority To Operate (ATO)

Derived from definitions in the IOT Cybersecurity Improvement Act of 202 and NIST SP 800-37r2



UFC 4-010-06 Cybersecurity for Facility-Related Controls

TETRA TECH

Mason&Hanger
A Day & Zimmermann Company

Most recently updated in OCT 23, the UFC provides design criteria to ensure cybersecurity policies are integrated into facility construction

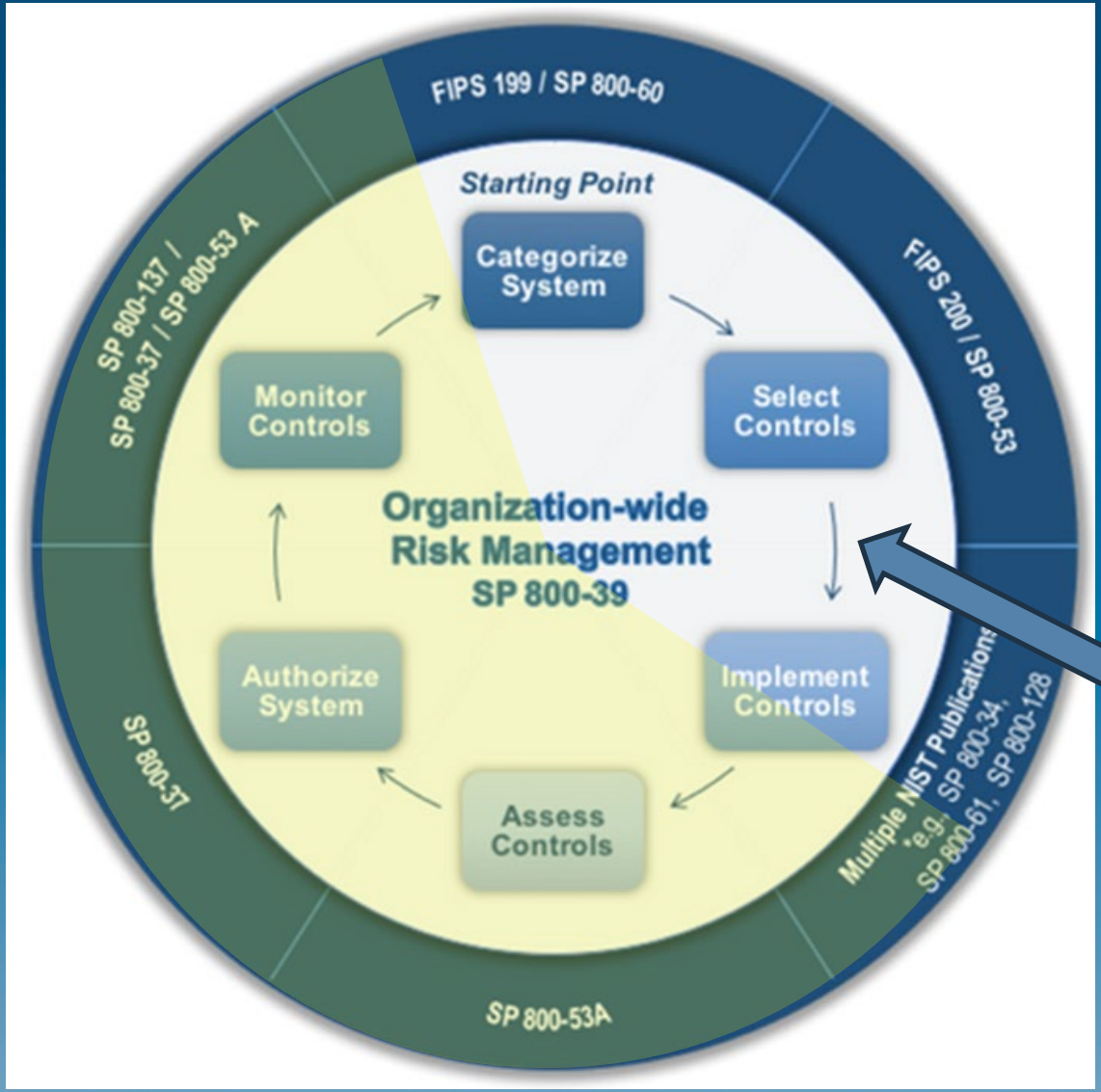
Derived from definitions in the IOT Cybersecurity Improvement Act of 202 and NIST SP 800-37r2

RMF and UFC 4-010-06

Differences between RMF and UFC 4-010-06

Aspect	NIST RMF	UFC 4-010-06
Primary Audience	Federal information systems and agencies	Department of Defense facilities and infrastructure
Focus	Information system cybersecurity risk management	Facility design and construction with integrated cybersecurity
Scope	System-level cybersecurity controls	Facility-level physical and cybersecurity security
Process Structure	Detailed steps for security control lifecycle	Integrated criteria for facility security design
Applicability	Broadly applicable across federal agencies	Specific to DoD facilities and infrastructure

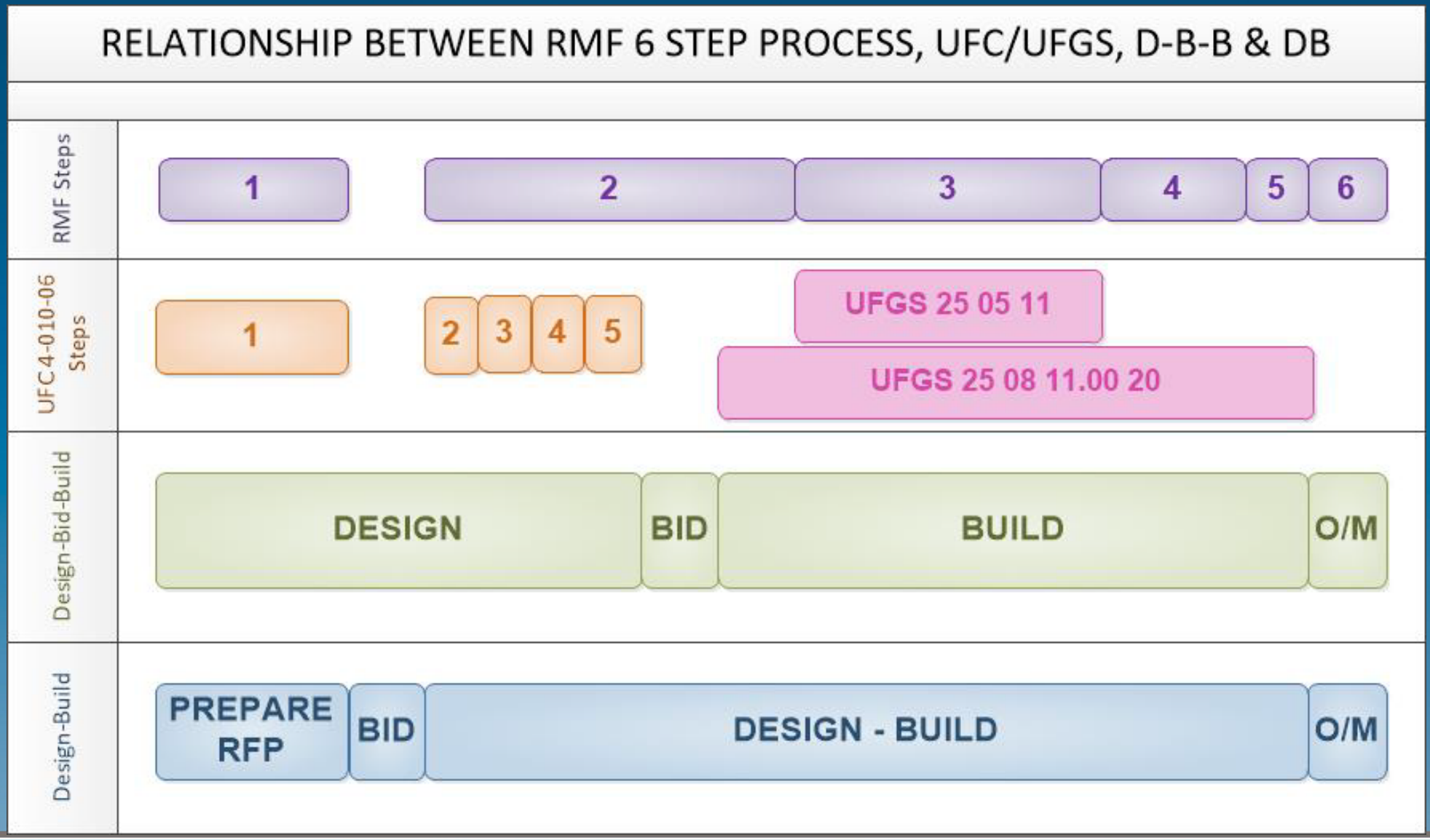
Risk Management Framework Steps



- Categorize System
- Select Controls
- Implement Controls
- Assess Controls
- Authorize System
- Continuous Monitoring

DESIGNER RESPONSIBLITY

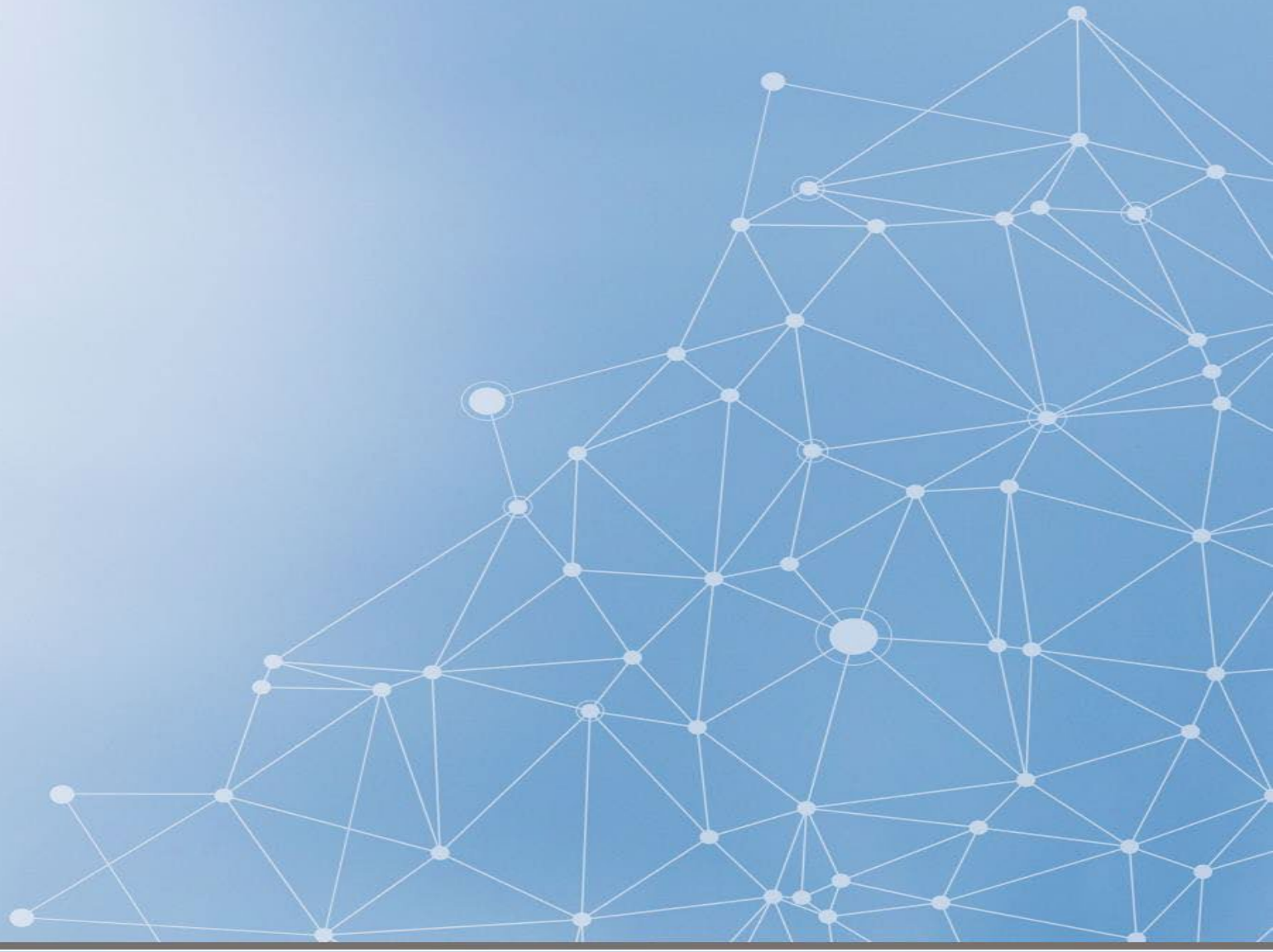
Execution: Process Alignment



TETRA TECH

Mason&Hanger
A Day & Zimmermann Company

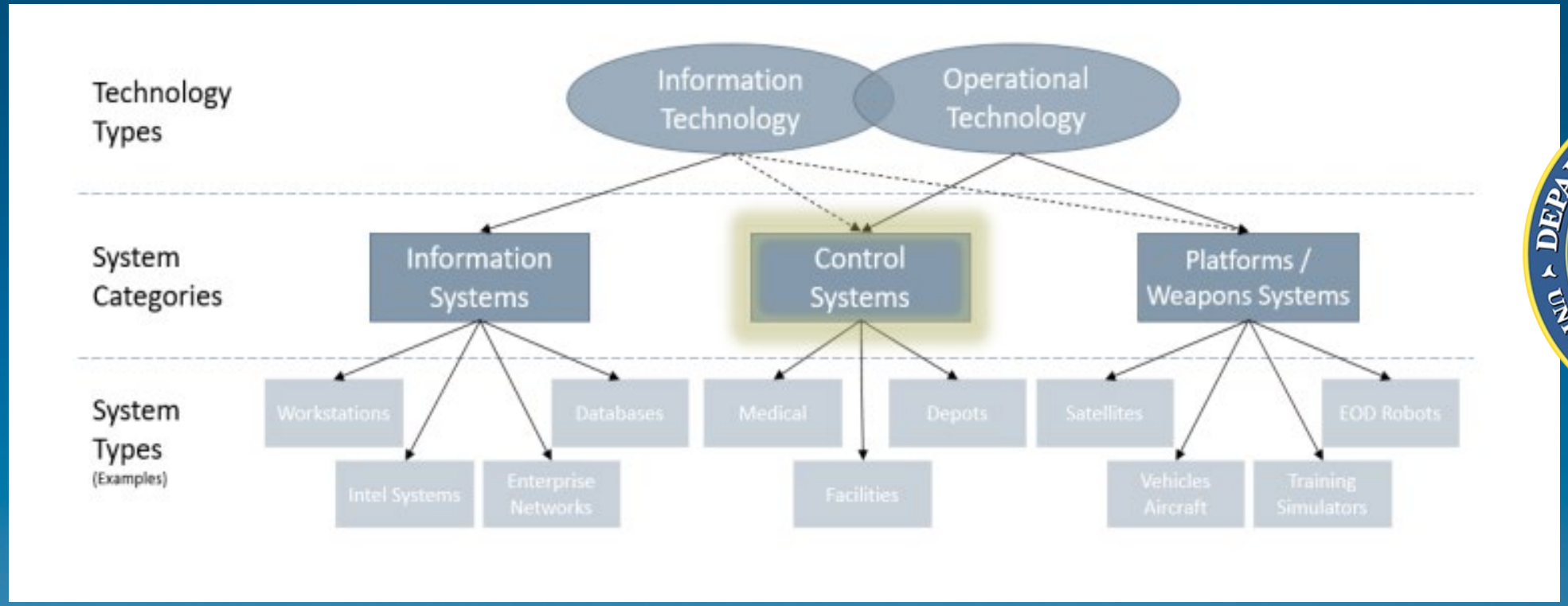
Cybersecurity in Facility Design and Construction



Applicability for Facility-Related Controls Systems (FRCS)

- **RMF: All new and active military construction projects must apply Risk Management Framework (RMF) and NIST Cybersecurity best practices**
- **UFC: Cybersecurity Assessment of projects must follow UFC 4-010-06, Cybersecurity Of Facility-Related Control Systems, October 10, 2023**
  - **Applicability:** Applies to all planning, design and construction, renovation, and repair of **new and existing facilities** (both permanent and non-permanent) and installations that result in DoD real property assets which include a control system with a network, regardless of funding source (and regardless of network type).

Cybersecurity for Facility-Related Controls



"Operational Technology has become ubiquitous and integrated into every piece of modern life. Throughout the DAF, control systems (a subset of operational technology) are extensively used to monitor, operate, and/or control equipment, infrastructure, and their associated devices (e.g., power generation and distribution, air conditioning, water and wastewater plants, natural gas distribution)." – DAFGM 2023-32-01, 27 June 2023

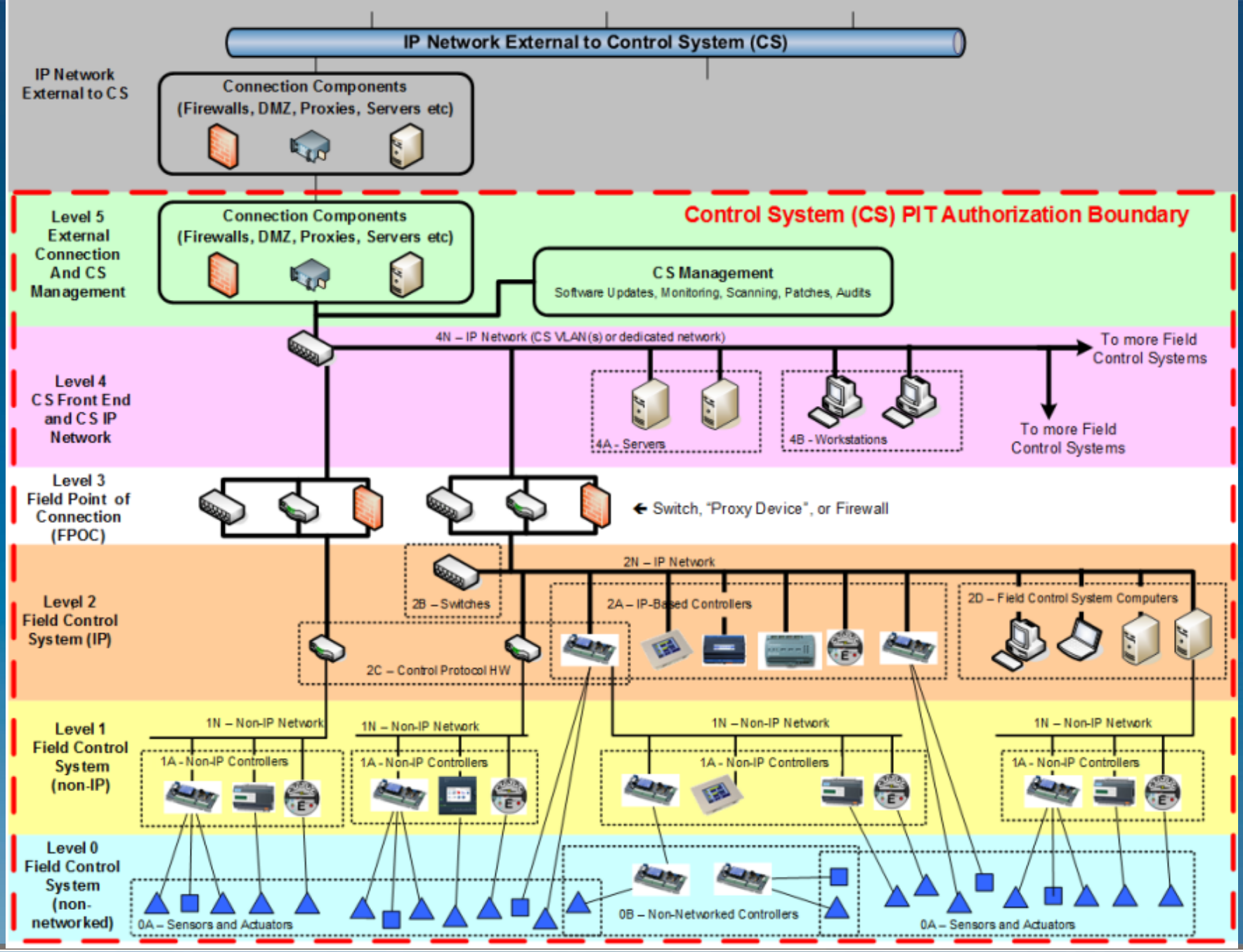
Facility-Related Control Systems (FRCS)

Applicable to all control systems installed in military and national security facilities but common facilities and infrastructure applications are:

- **Telecoms/Electrical**
  - Intrusion Detection System (IDS)
  - Access Control System (ACS)
  - Public Address (PA)
  - Closed-Circuit Television (CCTV)
  - Lighting
  - Airfield Lighting
  - SCADA
- **Fire & Life Safety (FLS)**
  - Fire Alarm/Suppression System
  - Mass Notification System (MNS)
- Mechanical
  - Building Automation Control System (BACS)
    - HVAC
  - Utility Monitoring Control System (UMCS)
  - Energy Monitoring Control System (EMCS)
  - Smart Meters (Gas, Water, Electric, Steam)
  - Conveyance

Full assessment

Assessment *may* not be needed



UFC 4-010-06 Assessment Process

Charrette Identification of All Contractor Furnished (CF) Equipment

- **Identify all Contractor-Furnished (CF) networked equipment (CF/CI or CF/GI)**
  - Anything “smarter than a piece of wire” that communicates needs to be identified, regardless of communication protocol
  - If a system is GF/GI, full cybersecurity assessment during design may not be required

Identify

- Computers
- Controllers
- Networked equipment
- Sensors
- Radio/Wireless

Follow-Up

- Location
- User Interfaces
- Communication Protocols
- Emergency Power (UPS)
- Physical Security (locked room, locked panels)
- External Connectivity

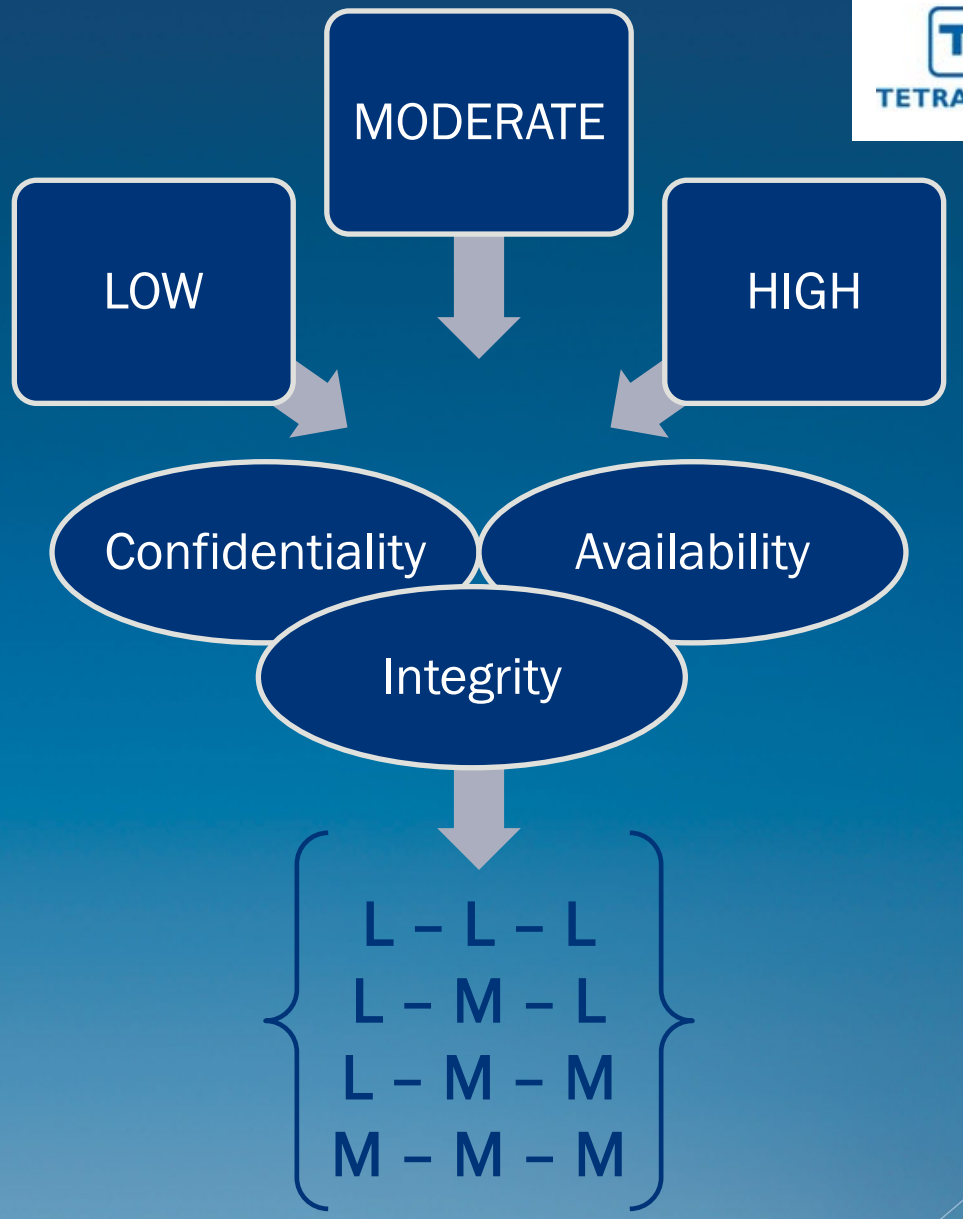
Cybersecurity Assessment Artifacts

- **Cybersecurity Design Analysis (DA) Section**
  - Summarizes physical and logical security controls for each control system
  - Tetra Tech products reference discipline-specific DA sections to minimize repeated information
- **Control Correlation Identifier (CCI) Tables - UPDATED**
  - Maps high-level policy statements (i.e., a security control) to discreet (low-level) security settings to determine compliance with stated objectives
  - Included as a DA attachment/appendix
  - Determine applicability of 909-1628 security controls per FRCS
- **UFGS Specification 25 05 11 – Updated on a recurring basis; cannot be templated without continuous update**
- **LATEST UPDATE AUG 2024**

Other discipline's DAs and specs must refer to the respective cybersecurity documents

C-I-A Ratings

- Request “Confidentiality-Integrity-Availability” Impact Rating for each FRCS between charrette meeting and charrette report
- Designation assigned by System Owner (SO) with concurrence from the Authorizing Official (AO)
- EXAMPLE: Fire Alarm confidentiality is a low criticality but availability is medium criticality; For an Instruction Detection System, C-I-A rating may be M-M-M across the board



CIA Ratings (Cont.)

- Identify Government Information System Owner (ISO) and Information Security System Manager (ISSM) PRIOR to Charrette
- **Provide the design team the Impact Ratings at the Charrette per UFC 4-010-06**
- When Impact Ratings can't yet be identified, ISO/ISSM must indicate one of the following for incorporation into the charrette report submittal:
  1. Use one of the categorization methods discussed in UFC 4-010-06 APPENDIX D to categorize the system for purposes of design and document how the categorization was determined.
  2. Design the system(s) to a L-L-L impact rating.
- Design Team cannot proceed with the design until C-I-A Impact ratings are provided
- Revision of App D or L-L-L assumptions that require rework are additional LOE after Charrette Deliverable has been accepted;
- Lack of determination at Charrette will delay submission of the Charrette Report, per UFC 4-010-06

What are CCIs?

- UFC classifies CCIs by implementation responsibility
- Often more than one party can implement a control, depending on the system characteristics

CCI-192: “The information system enforces password complexity by the minimum number of upper-case characters used.” is an enclave and designer control.

DoD-Defined

- May already be met by existing DoD policy

Non-Designer

- Typically the responsibility of the SO
- Beyond the design’s scope

Impractical

- Not able to be implemented on the FRCS

Enclave

- Assumed to be implemented on enclave (COINE) and can be inherited by the FRCS

Designer

- Must provide proof of implementation

NEW UFC 4-010-06 Requirements for 65% Design

If CCI *cannot* be incorporated

- Identification where and why the standard CCI requirements cannot be incorporated into the design
- Description of what requirements will be incorporated instead
- An explanation of the changes

If CCI *can* be incorporated

- Documentation of how the CCI has been incorporated into the control system design, including specification or drawing references.
- If there are specific changes from standard requirements, or multiple options available, document these changes or options.

CCI Examples

Control Number	CCI	CCI Definition	Implementation Guidance		Enclave	Designer	Non-Designer	Impractical	DoD-Defined	Not Applicable to FRCS	Justification for N/A to FRCS UFC Table G-2	Removed from Low baseline	Rationale for removal from Low baseline UFC Table G-3	UFGS 25 05 11 - Reference	
AC-18(3)	CCI-001449	The organization disables, when not intended for use, wireless networking capabilities internally embedded within information system components prior to issuance and deployment.	The organization being inspected/assessed documents and implements a process to disable wireless networking capabilities internally embedded within information system components prior to issuance and deployment when not intended for use.		X									---	

Recommendation for Government Management and Oversight of Cybersecurity Processes

- **Prior to Design Award:**
  - Step 1: Confirm if cybersecurity design of controls systems is applicable to the project
  - Step 2: Identify whether Community of Interest Network Enclave (COINE) or UMCS is available or planned installation dates, if any
  - Step 3: Always evaluate applicability of a Cybersecurity Specialist as Key Personnel in A-E teams
    - Required on most but not all projects
    - Early consultation can confirm applicability to specific project scope
  - Step 4: Identify Government Information System Owner (ISO) and Information Security System Manager (ISSM)

    (Note: The ISO and ISSM are NOT the Physical Security POC / SCIF SSO)
  - Step 5: Identify Facility-Related Controls Systems (FRCS) and C-I-A ratings PRIOR to Charrette
- **Design Execution – Steps 1 through 5 of UFC 4-010-06 (Section 3-1.1)**
  - Design Team to identify Control Systems; Government POCs to confirm
  - Government ISO must identify C-I-A Ratings for each system (**cannot be determined by A-E Team**)
  - Design Team to develop Draft and Final CCI Checklists for control systems; Government POC to review
  - For all Design Deliverables: Validate cost estimates and DD1391 include cybersecurity costs

TETRA TECH

Mason&Hanger
A Day & Zimmermann Company

Advancing Cybersecurity for the Future

Zero Trust Architecture (ZTA)

- **Zero Trust Principles:**

  "At its core, ZT assumes no implicit trust is granted to assets or users based solely on their physical or network location or asset ownership. Thid shift in philosophy is a significant change in legacy authentication and security mechanisms. It also represents a major cultural change that stakeholders will need to embrace and execute beginning with FY23 through FY27 and into the future"

- **DoD actively adopting ZTA for cybersecurity, including FRCS**
  - Continuous authentication and authorization of users, devices and systems accessing networks and physical access systems
  - Lead Privilege Access: access to facility systems is granted on a need-to-know and need-to-access
  - Micro-Segmentation: Facility controls are being segmented to isolate facility management systems from general IT networks
  - OT networks have a different cyber-physical network and zero trust principles apply differently

Cybersecurity for Facility-Related Controls

"Because of the increased reliance on systems within cyberspace under the Civil Engineer portfolio, the Civil Engineer community is a stakeholder (along with mission owners and cyber defenders) in mitigating the rising threats to infrastructure and supporting control systems as part of Civil Engineers' mission to establish, operate, maintain, and protect installations. Cyber risk management has become a critical element of Civil Eng."

– DAFGM 2023-32-01, 27 June 2023

Questions