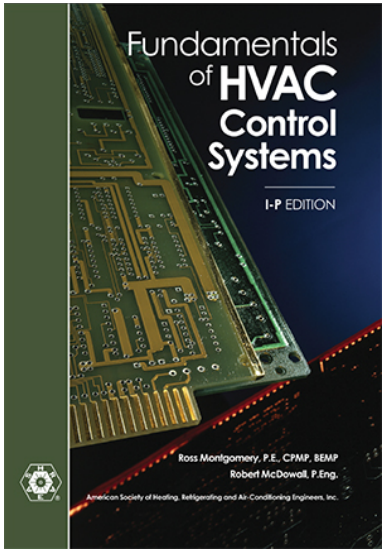
Navigating the Cybersecurity Hurdles of Design/Bid/Build + CMMC

Overview

- What is FRCS?
- Two Different Worlds Collide
- Government Challenges
- Tiny Piece of the A&E Pie
- What can be done?
- Why Cybersecurity Maturity Model Certification (CMMC)
- What are the focus areas of CMMC
- Current Timeline
- Impact and Responsibilities
- Danger of not implementing compliance

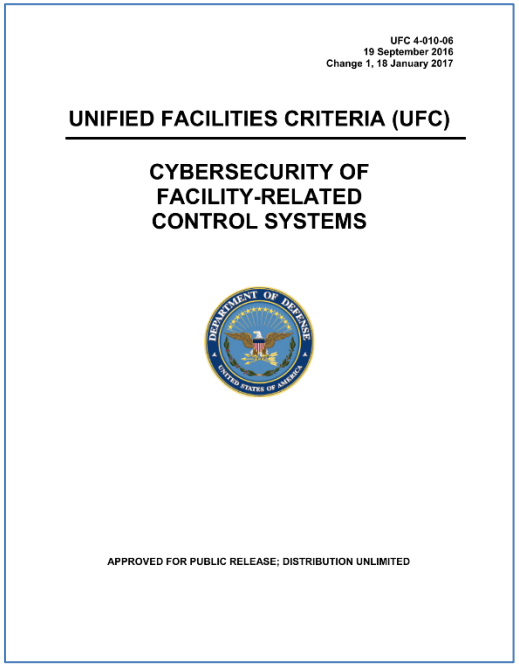
What is FRCS?

- Facility-Related Control Systems, aka “operational technology (OT)”
- Refers to control systems and their components used to monitor and control mechanical or electrical equipment/systems related to real property facilities
  - Examples – utility monitoring and control systems (UMCS), electronic security systems (ESS), building control systems (BCS), fire and life safety, and many more
- Can be connected to the internet and can contain or transmit sensitive or classified info, including PII
- Required to meet DoD Risk Management Framework (RMF) requirements and in some cases receive an Authority to Operate (ATO) – the process varies based on contract requirements and government expectations



What is FRCS cont..

- These systems are expected to be designed and hardened following standards and requirements published by NIST and CNSS – especially UFC 4-010-06 and UFGS 25-05-11
- However, these standards are often in a nascent phase and are not fully developed
  - UFC 4-010-06 applies to all new construction and repair projects, but only covers the design phase, not the whole project lifecycle
  - UFGS 25-05-11 guides the implementation of RMF for design and construction but is mostly geared towards HVAC and only in May 2021 has been expanded beyond low impact control systems


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

UNIFIED FACILITIES CRITERIA (UFC)

CYBERSECURITY OF FACILITY-RELATED CONTROL SYSTEMS

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

Two Different Worlds Collide

- Cybersecurity and A&E are markedly different
  - different timelines, different points of view, different technical standpoints, different languages
- Contract officers and those writing RFPs often seem unfamiliar with cybersecurity
  - I.E., references to outdated publications or specifications and requiring certain deliverables during the design phase that cannot be meaningfully produced until the build phase
- Contract language is frequently vague – often because an RFP is drafted years prior to project execution
- Updated publications, changing requirements, limited budgets, and differences of opinion between the contracting officer and end customer can further complicate issues

Government Challenges

- Government funding for FRCS cybersecurity is extremely disproportionate to the scale of the issue - while the number of DoD FRCS devices outnumbers traditional IT devices 250:1, only $1 is budgeted towards FRCS for every $200 for IT
- Getting RFI answers from the government is often a challenge in and of itself
  - Defining a system owner, CIA ratings of systems, or even the number of systems requiring FRCS deliverables can often take months, even a year+
  - H2L has encountered several times where the government has changed integral details of the system after contract award, often more than once, which have direct impact on the amount of effort required

Tiny Piece of the A&E Pie

- Those working in cybersecurity realize the importance of securing systems and the potential catastrophic effects that can result from a breach
- In the A&E world, cybersecurity might be only a small paragraph in a 1400 page RFP and cybersecurity labor might be represented by a few dozen hours along with thousands of other labor categories in proposal spreadsheets
- Cybersecurity is often an afterthought on complex design and build projects
    - H2L has experienced instances when the government has decided to nix cybersecurity completely during contract negotiations with an A&E firm
- While cybersecurity experts can voice the importance of incorporating cybersecurity in from the beginning of a project, like in other enterprise environments, it is often slapped on at the end as a quick fix solution

What can be done?

- Standardization of cybersecurity requirements throughout the different regions
- Agencies understanding the importance of cybersecurity
- Understanding the cost of implementing the cybersecurity controls
- Categorizing the system that is going to be assessed as soon as possible
- Communication, Communication, Communication

Transition

What's New in DFARS 252.204-

- What's new in DFARS and Its Impact: FederalRegister.gov/documents
  - DFARS 7012
    - Apply the security requirements of NIST 800-171 to Covered Contactor IS
  - DFARS 7019
    - ❖ Supplier Performance Risk System (SPRS) Requirements
    - Businesses must upload the NIST 800-171 Score
    - Contracting Office must review the SPRS prior to Award Contract
  - DFARS 7020
    - Requires contractors to provide the Gov. with access to facilities, systems, personnel to conduct CMMC assessment
  - DFARS 7021
    - ❖ Cybersecurity Maturity Model Certification
    - NLT September 30, 2025
    - Flow down to contractors

Why CMMC

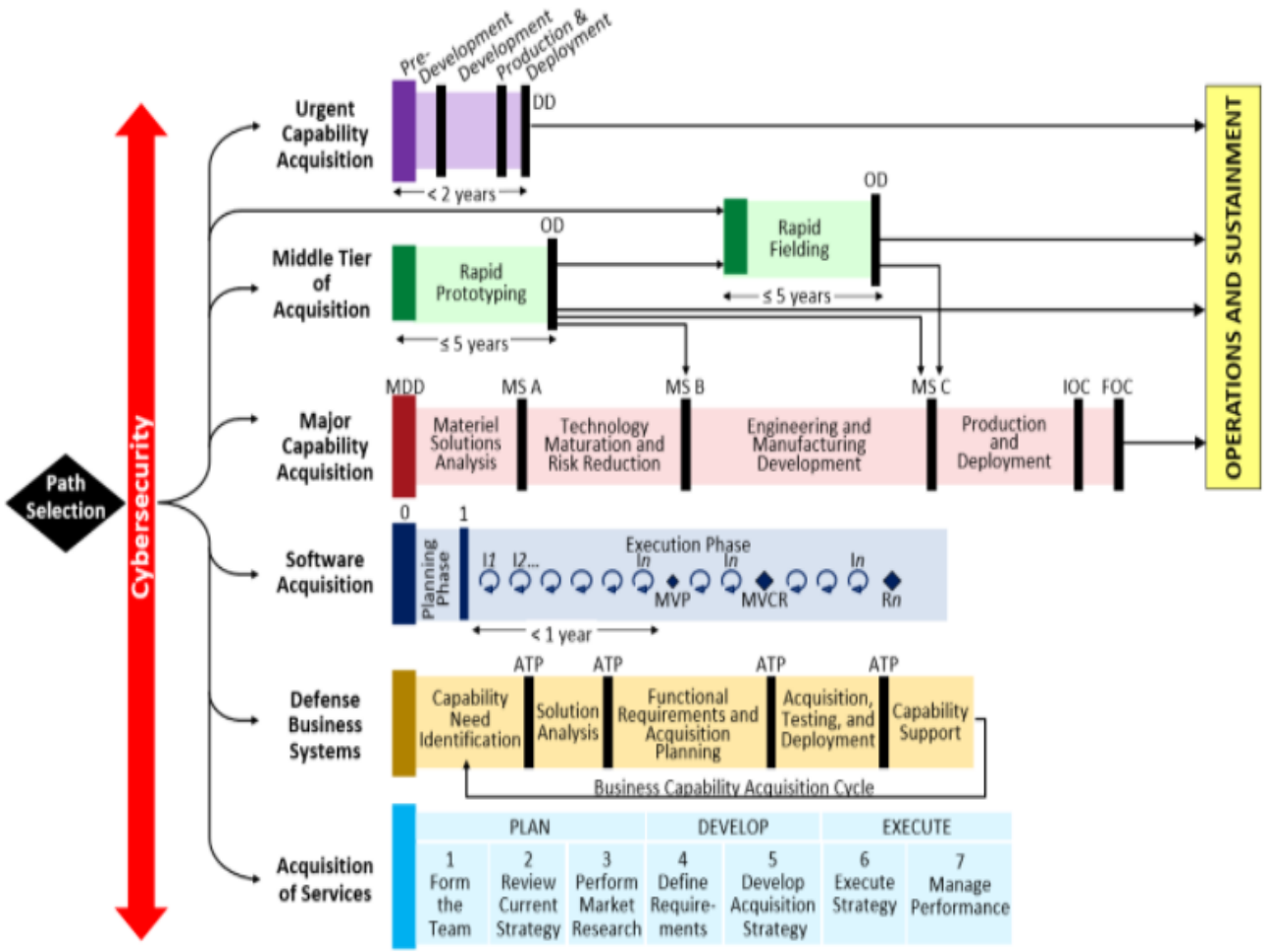
- Cybersecurity Maturity Model Certification (CMMC)
  - CMMC L1-Basic Cyber Hygiene
    - NIST 800-171 and CMMC 15 FAR Requirement
  - CMMC L2-Intermediate Cyber Hygiene
    - Steppingstone to L-3
  - CMMC L3-Good Cyber Hygiene
    - CUI Requirement
  - CMMC L4-ProActive
    - CUI Requirement
  - CMMC L5-Advanced/Progressive
    - CUI Requirement

CMMC-AB Focus Areas

- What are the Focus Areas
  - Obtaining Pool of Licensed Training Providers: Training and Certification Framework
  - Obtaining Pool of Licensed Partner Publishers: Develops Standard Curriculum

- Defense Acquisition University (DAU):
  - Adaptive Acquisition Framework-https://aaf.dau.edu/
  - Training
  - Implementing Clauses
  - Acquisitions Polices
    - **Overarching**
    - DoDD 5000.01 September 2020 The Defense Acquisition System
    - **Pathway**
    - DODI 5000.90 December 2020 Cybersecurity for Acquisitions
    - How to Tailor Programs
    - What needs to be protected
    - What CMMC Level does the data need to be protected

DAU: Adaptive Acquisition Framework



A set of acquisition pathways to enable the workforce to tailor strategies to deliver better solutions faster.

Jump to the Pathways

Help Me Select a Pathway

CMMC (Projected Rollout)

H2L SOLUTIONS

Total Number of New Prime Contracts Awarded Each Year with CMMC Requirements

FY 21	FY22	FY23	FY24	FY25
15	75	250	479	479

Total Number of Prime Contracts and Sub Contracts with CMMC Requirements

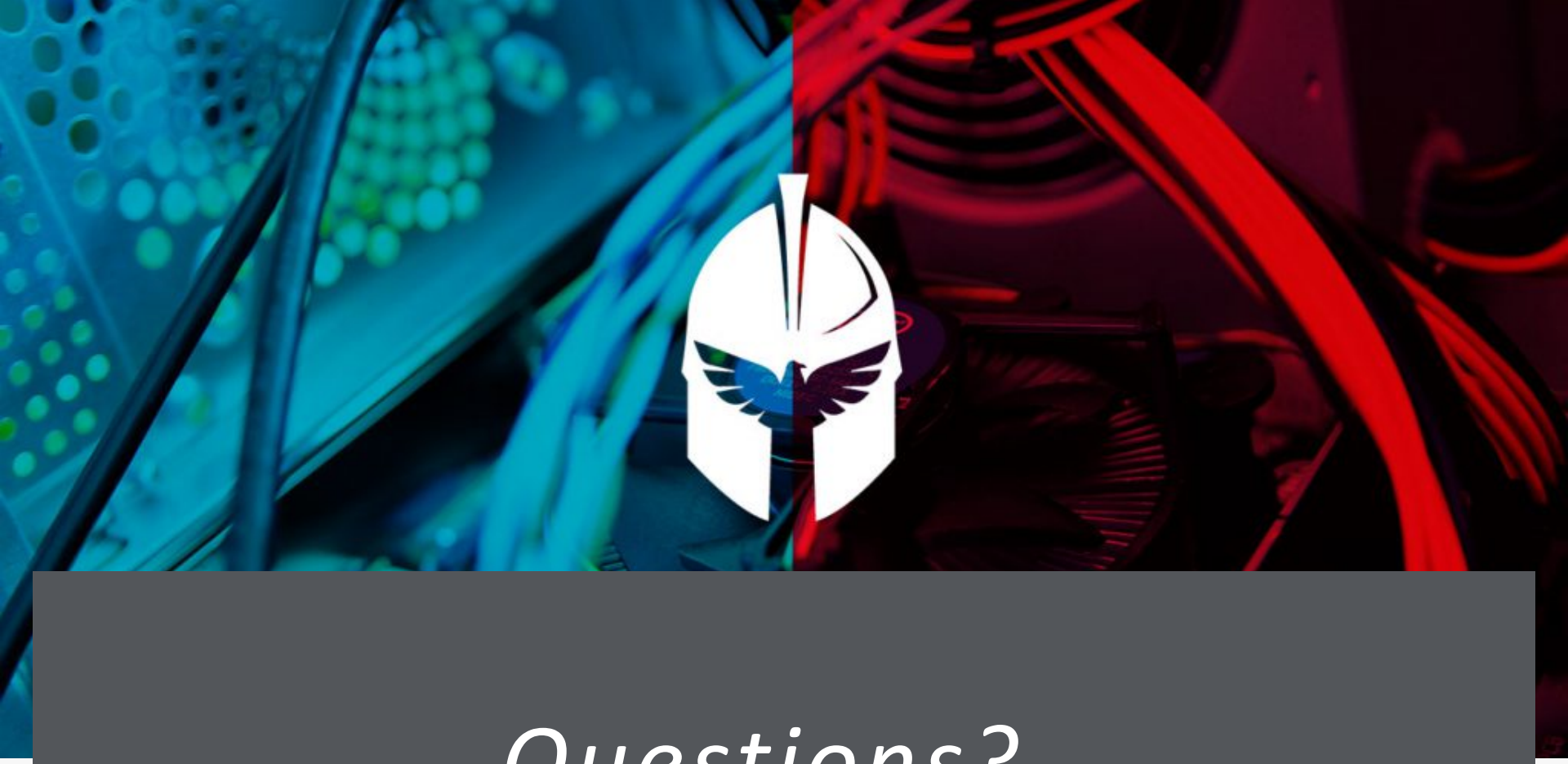
	FY21	FY22	FY23	FY24	FY25
Level 1	895	4,490	14,981	28,714	28,709
Level 2	149	748	2,497	4,788	4,785
Level 3	448	2,245	7,490	14,357	14,355
Level 4	4	8	16	24	28
Level 5	4	8	16	24	28
Total	1,500	7,500	25,000	47,905	47,905

Impact

- Impact
  - Cost
    - L1
    - L3
    - L4 and L5
  - Learning Curve
    - PM's, Contractors, Sub-Contractors
  - Sub-Contractors Uncertainty

Danger of Non-Compliance

- Not starting early enough
  - L-3 can take up to 1 year or longer
- Not able to complete
  - SPRS Score
  - Not Met
- Continued guidance
  - CMMC-AB still working on additional guidance



Questions?

H2L SOLUTIONS

For More Information

- Jonathan Hard
- Chief Executive Officer
- 256-679-9427
- Jonathan.Hard@H2LSolutions.com