FACILITY RELATED CONTROL SYSTEMS CYBERSECURITY

CONCEPTS TO ENABLE SUCCESSFUL PROJECT EXECUTION

U.S. Army Engineering and Support Center, Huntsville

Prepared by Daniel Shepard

August 2019

US Army Corps of Engineers

U.S.ARMY

BRIEFING OBJECTIVES

- High Level Snapshot of DoD & Army FRCS Cybersecurity Policy and Execution Timeline
- FRCS Unified Facility Criteria and Unified Facility Guide Specification Overview
- Key Considerations for Successful Project Execution

FACILITY-RELATED CONTROL SYSTEMS (FRCS)

- **FRCS consist of the control systems that operate Army facilities and represent a subset of a larger universe of control systems.**

- **FRCS are increasingly vulnerable to cyber attack due to greater network connectivity**

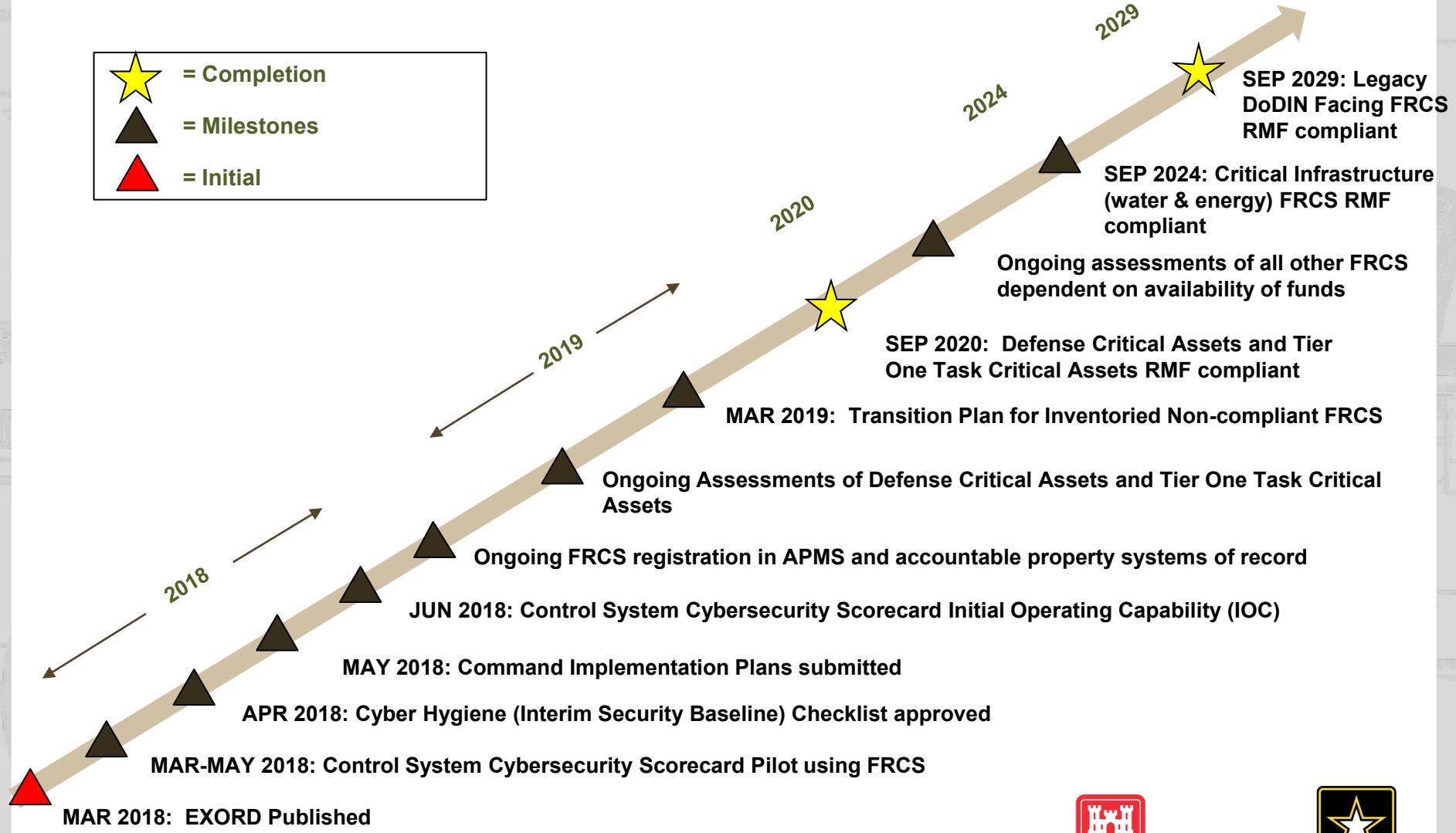
- **DoD and Army Policy Drivers**
  - 2014 DODI – Cybersecurity – Risk Management Framework (RMF)
  - 2015 Army Directive Risk Management Framework (RMF) for IT Systems
  - 2015 – ASA IEE directs IPT led by CIO-G6 for FRCS
  - 2016 – OSD Memo "Managing Cyber risks to FRCS
  - 2016 – UFC 4-010-06 Published
  - 2017 – UFGS 25 05 11 (Low Impact) Published
  - 2017 – Task Force Cyber Strong
  - 2018 – Army FRCS Cybersecurity Strategic Plan
  - 2018 – Army EXORD 141-18

Figure 1. Illustration of the Various Types of Facility-Related Control System

US Army Corps of Engineers

U.S.ARMY

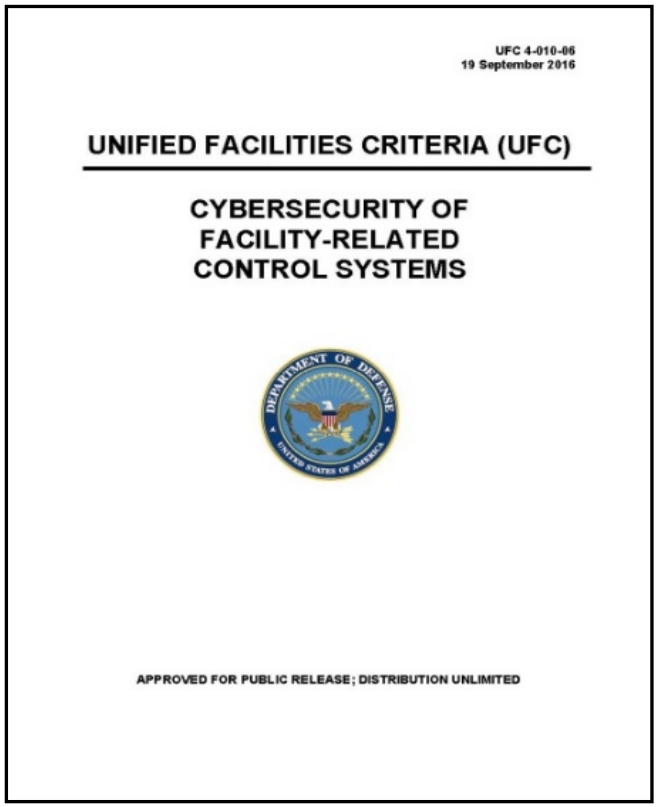
ARMY FRCS CYBERSECURITY EXECUTION TIMELINE



US Army Corps of Engineers

U.S.ARMY

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


UFC 4-010-06
19 September 2016

UNIFIED FACILITIES CRITERIA (UFC)

CYBERSECURITY OF FACILITY-RELATED CONTROL SYSTEMS

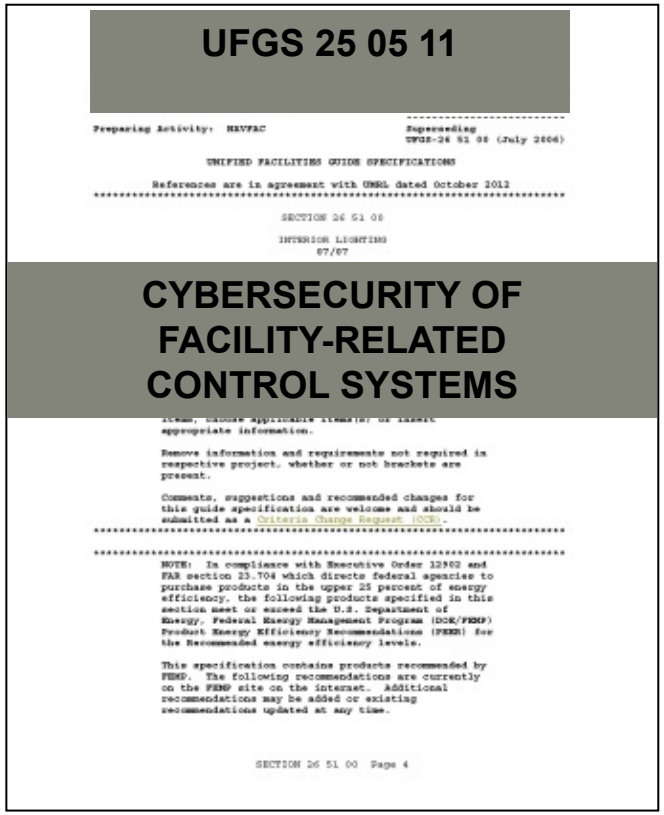
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

- Integrates the **DESIGNER** requirements supporting the Risk Management Framework (RMF) for facility-related control systems within design and construction projects. **DESIGNER** focused.
- Applies to all new construction and repair projects
- Published 19-September-2016
  - Whole Building Design Guide (www.wbdg.org)
- Relatively Narrow Focus – **DESIGN**, **NOT** life cycle (O&M)
  - Guidance to Designers-of-Record
  - Information from Designers-of-Record
- Impact System General Guidance
  - Details provided for **LOW** and **MODERATE** impact systems
  - ***HIGH*** impact systems require special attention

US Army Corps of Engineers

U.S.ARMY

UFGS 25 05 11 *CYBERSECURITY OF FACILITY-RELATED CONTROL SYSTEMS*


UFGS 25 05 11

Preparing Activity: NAVFAC

Superseding
UFGS-26 51 00 (July 2006)

UNIFIED FACILITIES GUIDE SPECIFICATIONS

References are in agreement with UMRL dated October 2013

SECTION 26 51 00

INTERIOR LIGHTING
07/07

CYBERSECURITY OF FACILITY-RELATED CONTROL SYSTEMS

appropriate information.

Remove information and requirements not required in respective project, whether or not brackets are present.

Comments, suggestions and recommended changes for this guide specification are welcome and should be submitted as a Criteria Change Request (CCR).

NOTE: In compliance with Executive Order 13502 and FAR section 23.704 which directs federal agencies to purchase products in the upper 25 percent of energy efficiency, the following products specified in this section meet or exceed the U.S. Department of Energy, Federal Energy Management Program (DOE/FEMP) Product Energy Efficiency Recommendations (PEER) for the Recommended energy efficiency levels.

This specification contains products recommended by FEMP. The following recommendations are currently on the FEMP site on the Internet. Additional recommendations may be added or existing recommendations updated at any time.

SECTION 26 51 00 Page 4

- Consolidated all FRCS cybersecurity submittals and related testing into one specification. Covers **LOW** Impact Systems
- Published November-2017
  - Whole Building Design Guide (www.wbdg.org)
- Includes requirements in support of the Risk Management Framework (RMF) for implementing cybersecurity into construction projects for facility-related control systems.

US Army Corps of Engineers

U.S.ARMY

UFGS 25 05 11: CYBERSECURITY FOR FACILITY-RELATED CONTROL SYSTEMS

- Covers **LOW** Impact Systems
- Update underway for **MODERATE** (Est. Publish Date 2nd Qtr. FY 20)
- Has to cover a ***wide*** range of systems and devices – ESS, HVAC, Fire, Elevator…
- Has tailored HVAC-specific requirements and "default" requirements for other systems
- Unfortunately, there's some big gaps with long designer notes of the "go figure it out" sort
- Includes submittals needed to support System Owner RMF Authorization Package

DIVISION OF RESPONSIBILITY, WHO OWNS THE PROBLEM??

- Multiple organizations are involved:
  - DPW/DES – system owner, operator, maintenance
  - NEC & R-NEC “Signal Brigade” – IP transport, C4IM Baseline Services
  - Building Tenant
  - Construction Agent
  - A/E Firm (DoR)
  - Potential of Multiple Authorizing Officials (System vs. Network)
- Different risks, different risk owners: Cyber risk, construction agent risk
  - Determination of roles & responsibilities up front are critical to project execution success .

US Army Corps of Engineers

U.S.ARMY

KEY CONSIDERATIONS

- Know who **OWNS** the FRCS (System Owner & RMF Authorization Official)

- Know the mission to which the FRCS is being designed to support and what is the IMPACT of the FRCS.
  - Not the designer's responsibility
  - Impact ratings provided by Government
    - Determined by SO in coordination with AO
    - But ***may*** have some give-and-take with designers to ensure that the delivery of a **FUNCTIONAL** system occurs.

- The UFC & UFGS is **NOT** RMF in its entirety.
  - System Shall (Design) vs. Organization Shall (O&M)

US Army Corps of Engineers

U.S.ARMY

KEY CONSIDERATIONS

- Ultimately cybersecurity requirements are “what the system owner and authorizing official are willing to accept” without impacting the functionality of the system to meet its purpose.
  - Remember we are **NOT** designing and constructing cybersecurity systems, we are designing and constructing FRCS’s.
  - Don’t create a tail wagging the dog situation.
- So we can assume “default” requirements, but ultimately need to design to the requirements of the System Owner and Authorizing Official
- This means we need to make sure to coordinate design with them early and often – more so than for other areas

KEY CONSIDERATIONS

- Contractors **CANNOT** provide an authorized system i.e. ATO, and we **SHOULD NEVER** give construction contractors general requirements like “meet cybersecurity”

- The design must define specific requirements, and those requirements must be met during construction and checked like any other requirement (Mechanical, Electrical, Structural, etc…)
  - UFGS defines the submittal schedule

- Specific contractual language is imperative to ensure success from both sides (Gov’t and Industry)
  - This is the entire focus of the UFGS

US Army Corps of Engineers

U.S.ARMY

QUESTIONS ?

US Army Corps of Engineers

U.S.ARMY