Control System

CYBERSECURITY EXPECTATIONS

05 April 2021

THIS TALK IS NOT ABOUT:

1. CMMC
   (Cybersecurity Maturity Model Certification)

2. RMF (Risk Management Framework)

3. Justifying the need for cybersecurity

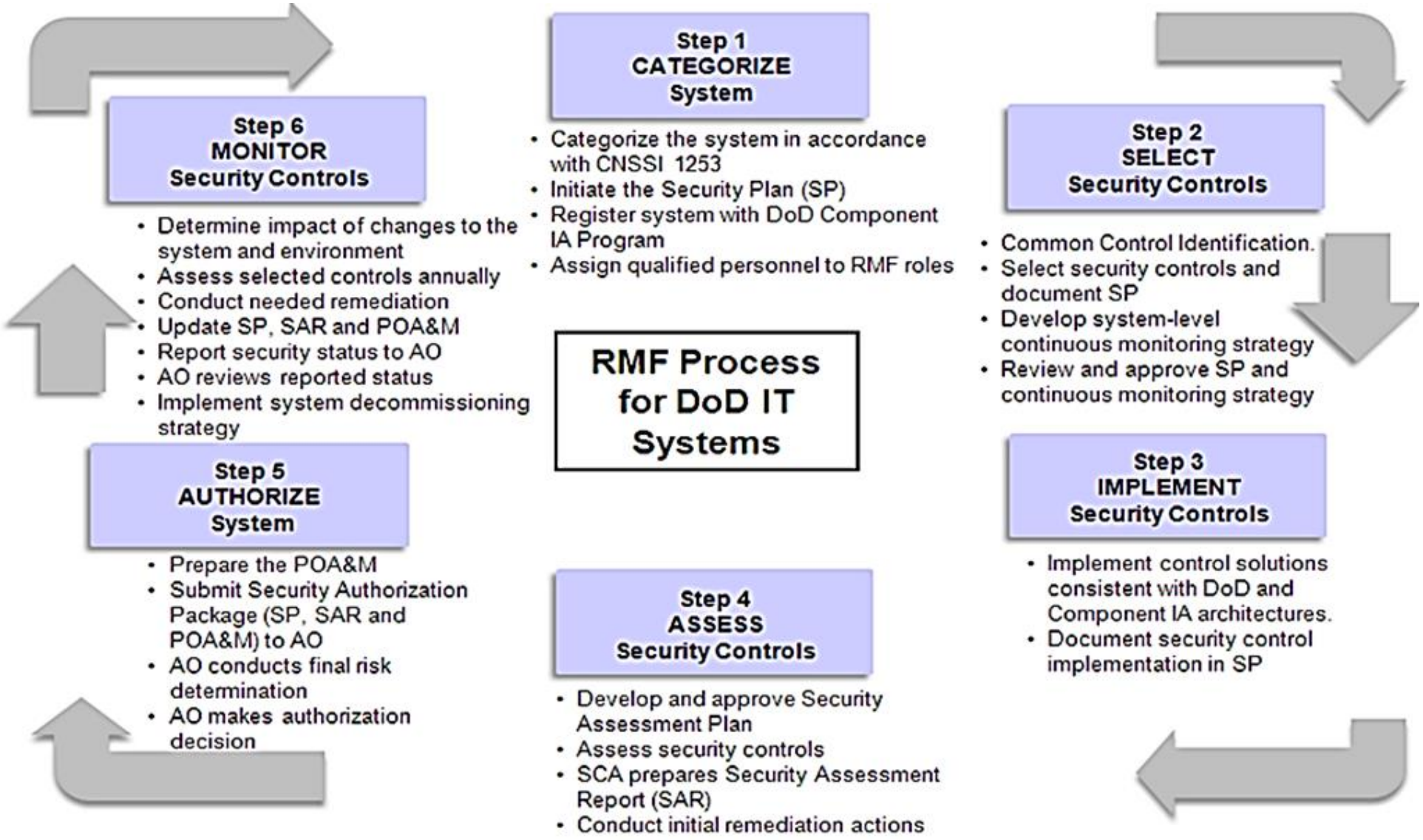
CMMC

- "How equipped are you to protect the government's data?"
- By 2026 all DoD contractors will need a CMMC certification
  - Only select 'pilot' contracts until 2026
  - Exception for COTS-only providers, but that's likely not you!
- Does not replace the existing DFARS .7012 requirement
- Level depends on CUI (Controlled Unclassified Information)
  - Level 1: You do not handle CUI, Level 3: You handle CUI

CMMC CONTINUED…

- CUI Includes Things Like…
  - Information on the Physical Security of DoD assets
  - Information on Vulnerabilities of Information Systems
- Personal Examples:
  - Drawings of security plans, Electronic Security System designs
  - ACAS Vulnerability Scan Results
  - Network Device Configuration Files
- This is a contracting/acquisition requirement
  - Talk to a Contracting Officer or check out YouTube!

RMF


Step 1
CATEGORIZE
System
• Categorize the system in accordance with CNSSI 1253
• Initiate the Security Plan (SP)
• Register system with DoD Component IA Program
• Assign qualified personnel to RMF roles
Step 2
SELECT
Security Controls
• Common Control Identification.
• Select security controls and document SP
• Develop system-level continuous monitoring strategy
• Review and approve SP and continuous monitoring strategy
RMF Process for DoD IT Systems
Step 3
IMPLEMENT
Security Controls
• Implement control solutions consistent with DoD and Component IA architectures.
• Document security control implementation in SP
Step 4
ASSESS
Security Controls
• Develop and approve Security Assessment Plan
• Assess security controls
• SCA prepares Security Assessment Report (SAR)
• Conduct initial remediation actions
Step 5
AUTHORIZE
System
• Prepare the POA&M
• Submit Security Authorization Package (SP, SAR and POA&M) to AO
• AO conducts final risk determination
• AO makes authorization decision
Step 6
MONITOR
Security Controls
• Determine impact of changes to the system and environment
• Assess selected controls annually
• Conduct needed remediation
• Update SP, SAR and POA&M
• Report security status to AO
• AO reviews reported status
• Implement system decommissioning strategy

JUSTIFYING THE NEED FOR CYBERSECURITY

2021 – Verkada Surveillance Cameras & Access Control

2021 – Florida Water Plant Hack

2020 – SolarWinds Hack

2020 - 50,000 IP-based surveillance cameras hacked

2019 – First US electrical utility disrupted by cyberattack

2016 – Ukraine power devices hack: 60 substations (Russia)

2018 – Saipem (Italian oil) crippled by cyberattack

2015 – Ukraine power operators PC: 250k customers(Russia)

2015 – Turkey electrical distribution (Iran suspected)

2014 – Wastewater plant, Alliant Healthcare, Sony

2013 – Bowman Dam (NY) Hack

THIS TALK IS ABOUT:

1. Goals of Cybersecurity in DoD Control System Construction

2. DoD Control System Cybersecurity Construction Guidelines

   - Design Requirements and Expectations
   - Key Construction Submittals

GOALS IN DOD Control System DESIGN/CONSTRUCTION:

#1: Meet the functional requirements.

- Tailor cybersecurity requirements to the project.
  - Example: If the customer doesn't need a redundant system, the cybersecurity controls shouldn't prescribe one.

- Keep it simple.
  - If you can meet the requirements without a "smart system", do so.
  - We can't afford to secure and continuously monitor unnecessary systems.

GOALS IN DOD Control System DESIGN/CONSTRUCTION:

#2: Provide a secured/hardened system.

- Goal **IS NOT** to get an ATO (Authority to Operate)
- Goal **IS** to provide a secured system with supporting documentation so that the system is technically capable of receiving an ATO without the need for reconfiguration.

Control System V

DOD CYBERSECURITY CONSTRUCTION GUIDELINES

UFC 4-010-06 & UFGS 25 05 11

- UFC: Cybersecurity of Facility-Related Control Systems
  - Revision likely released in Summer 2021.
  - Minimize Network Dependency
  - Reduce Extraneous Functionality
  - Design for Graceful Failure
  - No Remote Access!

- UFGS: Must be tailored to the system!
  - Revision anticipated to be released in May 2021.

DESIGN REQUIREMENTS & EXPECTATIONS

Step 1: Determine the System's Impact Rating [Categorization]

Cybersecurity: Practices designed to protect the **confidentiality, integrity,** and **availability** of information systems and data.

C-I-A (aka "Impact Rating")

L-M-H (Low – Moderate – High)

DESIGN REQUIREMENTS & EXPECTATIONS

Step 1: Determine the System's Impact Rating [Categorization]

- This is the customer's responsibility!
  - Ideally, this is defined during the 1391 development…unfortunately, we're not there yet.
  - If a rating is not provided [for each system], submit an RFI.
  - If they fail to respond, document that in the Design Analysis (DA) and make an assumption.
    - Assumption may be based on the "FRCS Master List", similar past projects, or guidance from the MCX.
  - Each system's impact rating and how it was obtained should be documented in the DA.

Note: *If you're modifying, or connecting to, an existing system, there is a [small, but growing] chance that an ATO exists for that system. If so, then there will be an already approved Impact Rating and baseline CCIs. It should also define how changes are to be made to the system.*

DESIGN REQUIREMENTS & EXPECTATIONS

Step 2: Generate the list of *potentially* applicable controls.

- You could start with the Controls (UFC 4-010-06, Appendix G)
- Often simpler to jump to the CCIs (Control Correlation Identifiers)
  - UFC 4-010-06, Appendix H tells you which CCIs do, or do not, apply to Control Systems.
  - Also tells you which CCIs are, or are not, the designer's responsibility.
  - Also tells you at what impact level specific CCIs apply to (LOW or MODERATE).
  - After filtering these down, this is your **baseline** CCI set.
    - SAVE THESE BASELINES AS STARTING POINTS FOR OTHER SIMILAR PROJECTS!

DESIGN REQUIREMENTS & EXPECTATIONS

Step 3: Start tailoring the applicable CCIs.

- At 35% you might not know everything, but use what you know:
  - A hard requirement for a workstation will drive many 'Applicable' CCIs
  - A basic Fire Alarm Panel will have relatively few

- Continue to tailor this list as the design progresses.
  - Maintain close communications with the other disciplines

DESIGN REQUIREMENTS & EXPECTATIONS

Step 3: Start tailoring the applicable CCIs.

CCI	Control Text (Summarized)	Fire Alarm Panel	Full BAS w/PC
CCI-000399	Produce an Inventory	Applicable	Applicable
CCI-000200	Passwords can't be reused for at least 5 generations.	Impractical	Applicable
CCI-001989	Change Default Credentials	Applicable	Applicable
CCI-001441	Maintain Audit Trail on Wireless Access	N/A*	N/A*

DESIGN REQUIREMENTS & EXPECTATIONS

Step 4: Start tailoring the 25 05 11 specification.

- Every paragraph in the 25 05 11 is tied to one or more CCIs
  - Eliminate the paragraphs for 'N/A' or 'Impractical' CCIs

```
3.1.1   System Use Notification

 {For Reference Only:  This subpart (and its subparts) relates to AC-8;
 CCI-000048, CCI-002247, CCI-002243, CCI-002244, CCI-002245, CCI-002246,
 CCI-000050, CCI-002248}

 Web interfaces must display a warning banner meeting the requirements of
 DTM 08-060.
```

- Include any site or system-specific requirements.
  - Ex. An existing ATO's Configuration Management requirements
  - Ex. The office/department responsible for issuing IP addresses.

DESIGN REQUIREMENTS & EXPECTATIONS

What are you really looking for?

DESIGN REQUIREMENTS & EXPECTATIONS

Concept Design Expectations (10-35%)

- Separate Cybersecurity chapter in the DA
  - Provide functional description/narrative of each system, plus:
    - System's impact rating and how it was determined.
    - Interconnection requirements and responsibilities.
    - Any existing ATOs and/or specific Configuration Management requirements
    - **Preliminary CCI lists based on the impact rating and known system attributes**
  - Provide a High-Level/Notional Diagram*
    - *Not technically required by the UFC…yet…but…

- UFGS: Table of Contents
  - One 25 05 11 entry for each control system*
    - Significantly similar systems may be combined

DESIGN REQUIREMENTS & EXPECTATIONS

Design Development Expectations (50-65%)

- Updated DA that is consistent across disciplines and drawings
  - CCI lists are relatively finalized and properly annotated.
    - (Each CCI either indicated as incorporated into the design, or a reason given for its exclusion.)
  - Any basis-of-design cut sheets provided align with the cybersecurity approach.
    - (Don't include a cut sheet for an Air Compressor that comes standard with an integrated webserver!)
- Draft 25 05 11 specification for each system
  - 25 05 11 is generally tailored to the specific control system (in accordance with CCIs)
  - There are no inconsistencies between the 25 05 11 and other specs/drawings

DESIGN REQUIREMENTS & EXPECTATIONS

Pre-Final Design Expectations (90-95%)

- Each 25 05 11 is complete and fully tailored to each system.
  - The CCIs are finalized and fully incorporated into the specs
  - "N/A" or "Impractical" CCIs have been removed from the specs
  - No inconsistencies between spec sections
  - No inconsistencies between the 25 05 11 and the drawings

CONSTRUCTION REQUIREMENTS

There's a 25 05 11; what do I do with it?

- The intent of the 25 05 11 was to eliminate the need for a cybersecurity SME. However…
  - The specification relies heavily on "STIG/SRGs"
  - Throws out terms like "Vulnerability Scanning"
  - Specific devices are not often known at time of design

KEY 25 05 11 SUBMITTALS

SD-01 Pre-Construction

- Contractor Cybersecurity Compliance Statements
- Cybersecurity Subject Matter Expert Qualifications*

SD-02 Shop Drawings

- Network Communication Report (Ports & Protocols)
- Cybersecurity Riser Diagram
- Control System Inventory Report
- Cybersecurity Interconnection Schedule
- Proposed STIG/SRGs*

KEY 25 05 11 SUBMITTALS

SD-03 Product Data

- Control System Cybersecurity Documentation
  - Technical Manual (user roles, permission matrix, security options)
  - Vendor Secure Configuration/Installation Guides
  - Known vulnerabilities (vendor releases, ICS-CERT, NIST NVD)

SD-11 Closeout Submittals

- Password Summary Report
- Software Recovery and Reconstitution Images (Backups)
- Completed STIG/SRG Checklists*
- Completed Vulnerability Scans*

ANTICIPATED REVISIONS TO UFGS 25 05 11

- Software disabling of Wireless is not sufficient, must be physical.
- Defining customer POCs in the specs (improved coordination).
- New submittals: Proposed STIG/SRGs, Test Procedures, Maintenance Tool Software, Scanning Tools, Information at Rest, Integrity Verification, Software/Configuration Backups
- Additional spec tailoring options:
  - Controllers, Lighting Control, ESS, Fire Protection
- Support for MODERATE systems.

</TALK>

Cybersecurity requirements depend on the specific system.

Cybersecurity is not just technical controls.