SAME Omaha Post
UFC-4-010-06
Requirements Overview

HDR

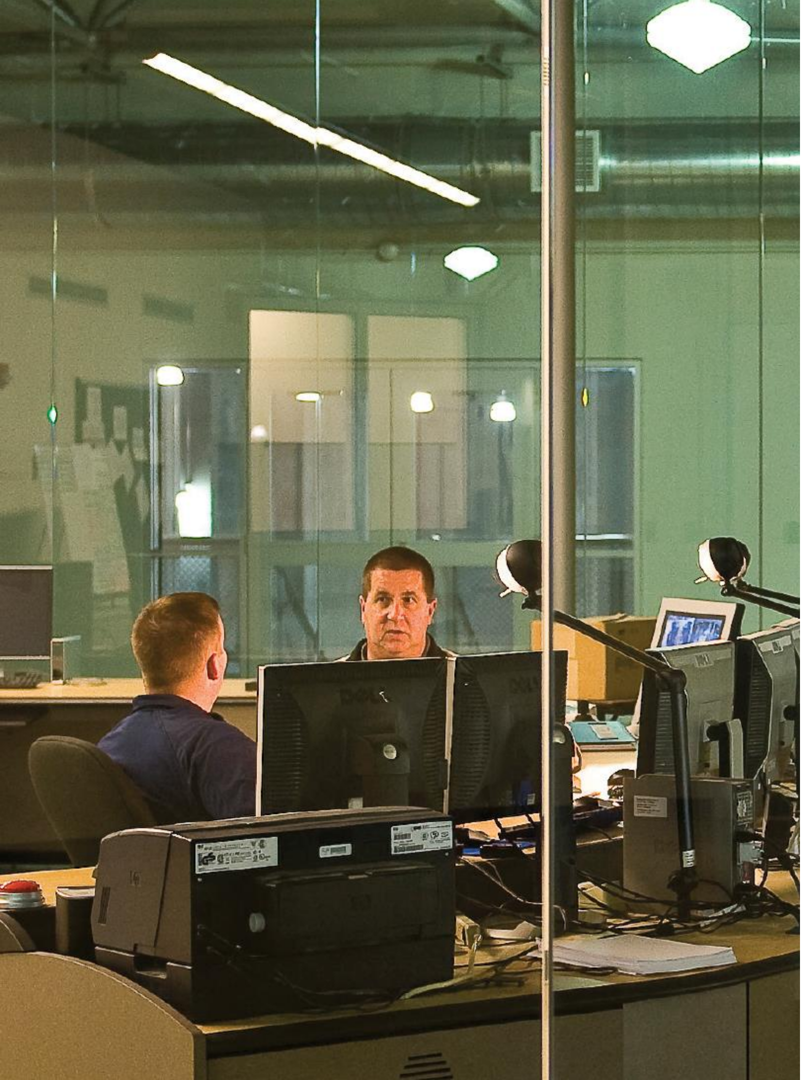
January 14, 2021

Presenter

David Brearley, GICSP, PMP

Program Manager, Cybersecurity

David.Brearley@hdrinc.com



AGENDA

01 The Why

02 The What

03 The How

04 Costs

05 Q&A

01 The Why

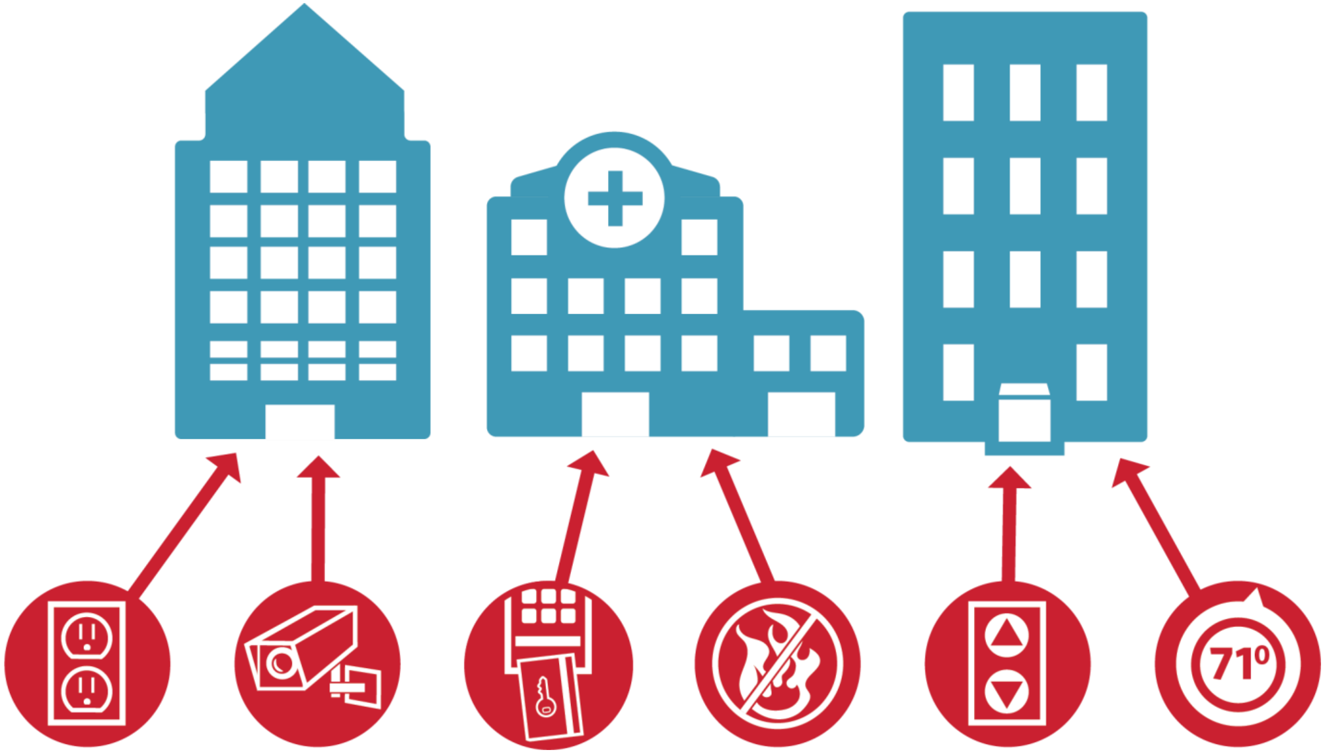
Presidential Policy Directive 21 (PPD-21):

Critical Infrastructure Security and Resilience

Defines 16 Critical Infrastructure Sectors

- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Food & Agriculture
- Dams
- Defense Industrial Base
- Emergency Services
- Energy Sector
- Financial Services
- Food & Agriculture
- Government Facilities
- Healthcare
- IT
- Nuclear

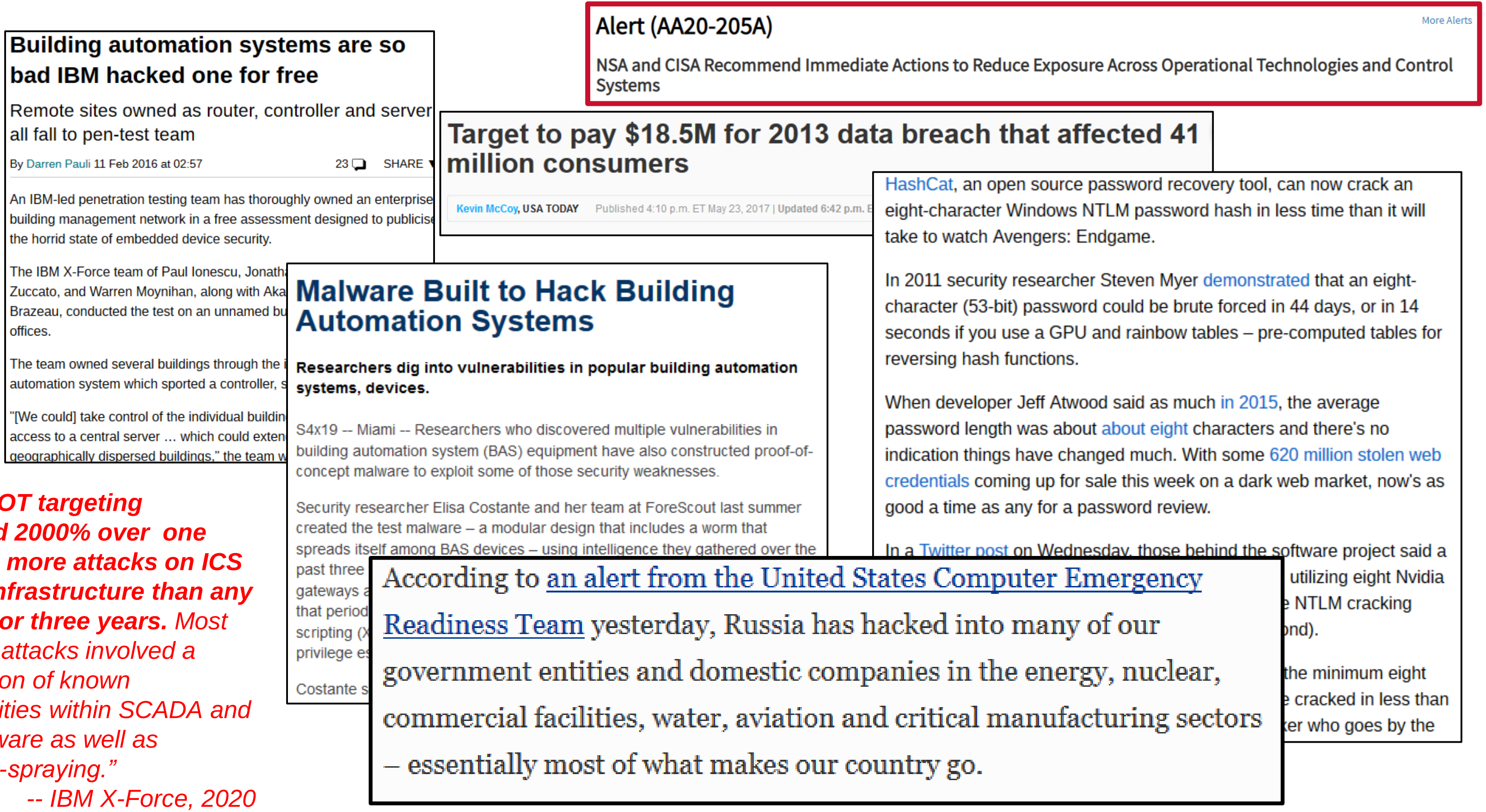
Cybersecurity Threats to Critical Infrastructure



Cybersecurity Threats to Energy/Power

Cybersecurity Threats to Energy/Power

Cybersecurity Threats to Critical Infrastructure



Alert (AA20-205A)

More Alerts

NSA and CISA Recommend Immediate Actions to Reduce Exposure Across Operational Technologies and Control Systems

Building automation systems are so bad IBM hacked one for free

Remote sites owned as router, controller and server all fall to pen-test team

By Darren Pauli 11 Feb 2016 at 02:57

23 SHARE

An IBM-led penetration testing team has thoroughly owned an enterprise building management network in a free assessment designed to publicise the horrid state of embedded device security.

The IBM X-Force team of Paul Ionescu, Jonath Zuccato, and Warren Moynihan, along with Aka Brazeau, conducted the test on an unnamed bu offices.

The team owned several buildings through the i automation system which sported a controller, s

"[We could] take control of the individual buildin access to a central server … which could exten geographically dispersed buildings," the team w

Target to pay $18.5M for 2013 data breach that affected 41 million consumers

Kevin McCoy, USA TODAY Published 4:10 p.m. ET May 23, 2017 | Updated 6:42 p.m. E

HashCat, an open source password recovery tool, can now crack an eight-character Windows NTLM password hash in less time than it will take to watch Avengers: Endgame.

In 2011 security researcher Steven Myer demonstrated that an eight-character (53-bit) password could be brute forced in 44 days, or in 14 seconds if you use a GPU and rainbow tables – pre-computed tables for reversing hash functions.

When developer Jeff Atwood said as much in 2015, the average password length was about about eight characters and there's no indication things have changed much. With some 620 million stolen web credentials coming up for sale this week on a dark web market, now's as good a time as any for a password review.

In a Twitter post on Wednesday, those behind the software project said a utilizing eight Nvidia e NTLM cracking ond).

the minimum eight e cracked in less than ker who goes by the

Malware Built to Hack Building Automation Systems

Researchers dig into vulnerabilities in popular building automation systems, devices.

S4x19 -- Miami -- Researchers who discovered multiple vulnerabilities in building automation system (BAS) equipment have also constructed proof-of-concept malware to exploit some of those security weaknesses.

Security researcher Elisa Costante and her team at ForeScout last summer created the test malware – a modular design that includes a worm that spreads itself among BAS devices – using intelligence they gathered over the past three gateways a that period scripting (X privilege es

Costante s

According to an alert from the United States Computer Emergency Readiness Team yesterday, Russia has hacked into many of our government entities and domestic companies in the energy, nuclear, commercial facilities, water, aviation and critical manufacturing sectors – essentially most of what makes our country go.

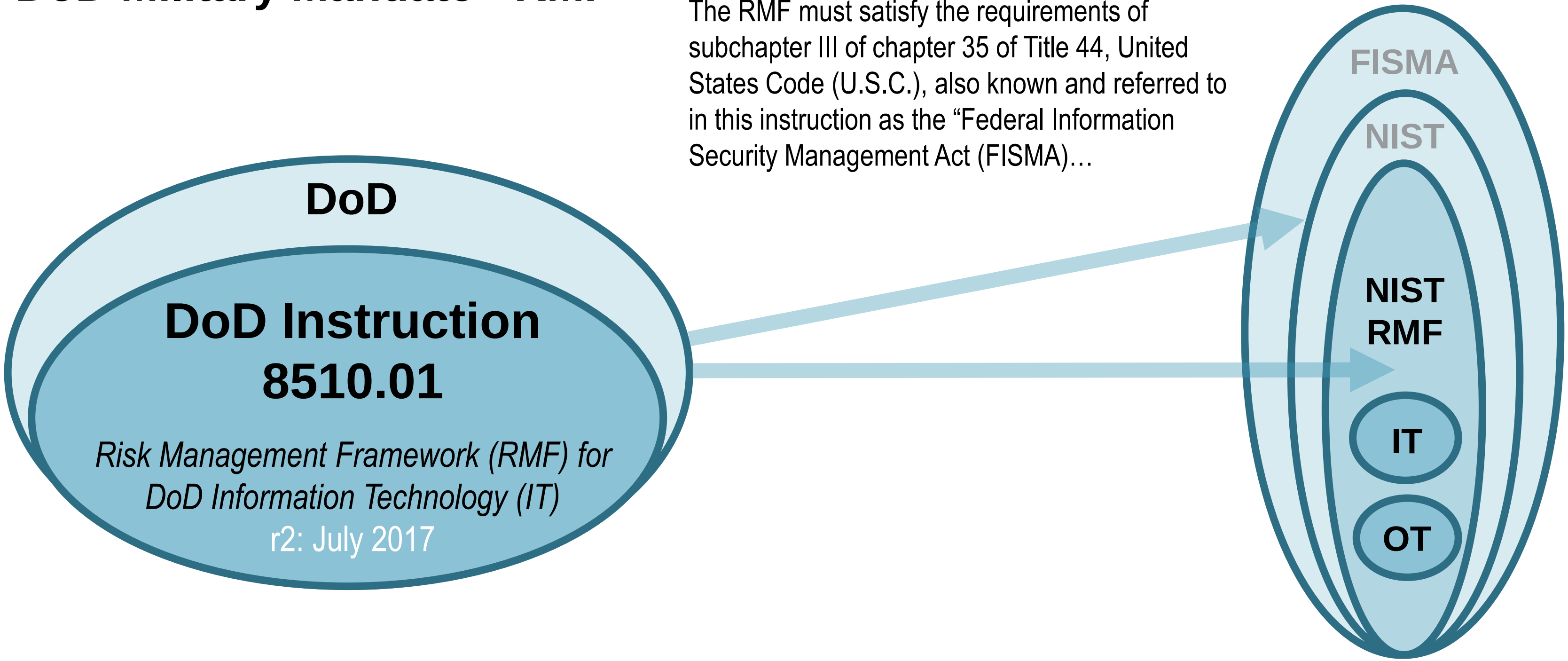
"In 2019, ***OT targeting increased 2000% over one year with more attacks on ICS and OT infrastructure than any of the prior three years.*** *Most observed attacks involved a combination of known vulnerabilities within SCADA and ICS hardware as well as password-spraying."*

-- IBM X-Force, 2020

02 The What

DoD Military Mandate - RMF

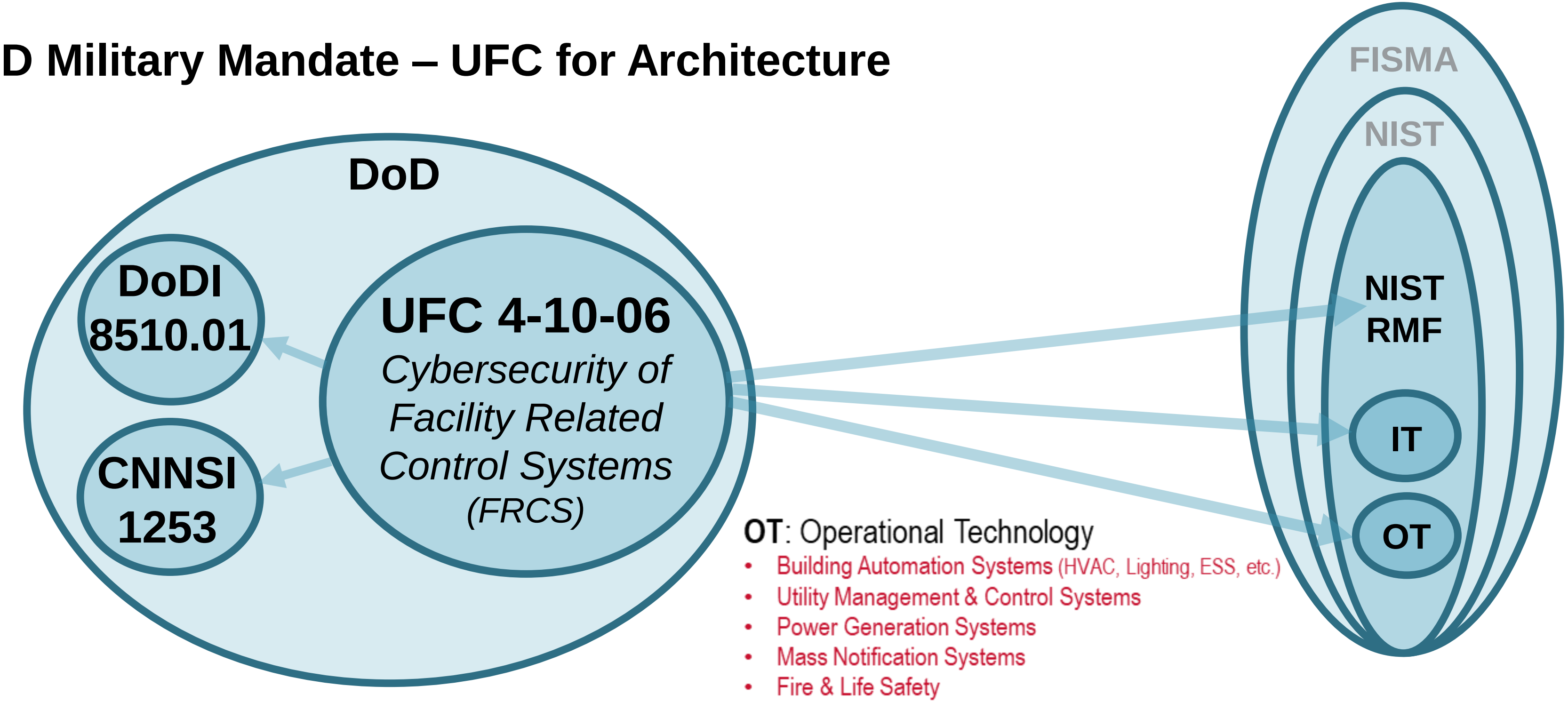
The RMF must satisfy the requirements of subchapter III of chapter 35 of Title 44, United States Code (U.S.C.), also known and referred to in this instruction as the “Federal Information Security Management Act (FISMA)…


DoD
DoD Instruction 8510.01
Risk Management Framework (RMF) for DoD Information Technology (IT)
r2: July 2017
FISMA
NIST
NIST RMF
IT
OT

The cybersecurity requirements for DoD information technologies will be managed through the RMF consistent with the principals established in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 (Reference (c)). DoD IS and **PIT** systems will transition to the RMF in accordance with…

PIT: Platform Informational Technology = Military OT

DoD Military Mandate – UFC for Architecture



OT: Operational Technology

- Building Automation Systems (HVAC, Lighting, ESS, etc.)
- Utility Management & Control Systems
- Power Generation Systems
- Mass Notification Systems
- Fire & Life Safety

Description: UFC 4-010-06 provides requirements for incorporating cybersecurity into the design of facility-related control systems.

This UFC provides criteria for the inclusion of cybersecurity in the design of control systems in order to address appropriate Risk Management Framework (RMF) security controls **during design and subsequent construction**.

Facility Related Control Systems (FRCS)

- Electronic – ESS (Government Furnished)
  - Intrusion Detection System (IDS)
  - Physical Access Control System (PACS)
  - Video/CCTV (CCTV)
- Fire & Life Safety (FLS)
  - Fire Alarm Reporting System (FARS)
  - Fire Suppression System (FSS)
  - Mass Notification System (MNS)
- Utility Monitoring and Control System (UMCS)
  - Building Control System (BCS) ** integrated into UMCS
    - Building Automation System (BAS)
    - Building Lighting System (BLS)
    - Electrical System (ES)
    - Water Meters
    - Heating, Ventilation, Air Conditioning (HVAC)
      - Subsystems: Boilers/Chillers/Chemical Treatment/Cooling Tower/Hydronic Pumps
- Utility Control (UCS)
  - Enterprise Energy Data Reporting System (EEDRS) – Electric/Gas Meters

Applies to any intelligent (programmable) system provided or modified by contractor.

The What Summary:

DoD

- All new and active projects must apply RMF and NIST cybersecurity best practices
- All infrastructure projects must follow UFC 4-010-06

Federal

- All new and active projects must apply RMF and NIST minimum requirements

SECURITY: Grid regulator hits utility with record $10M fine

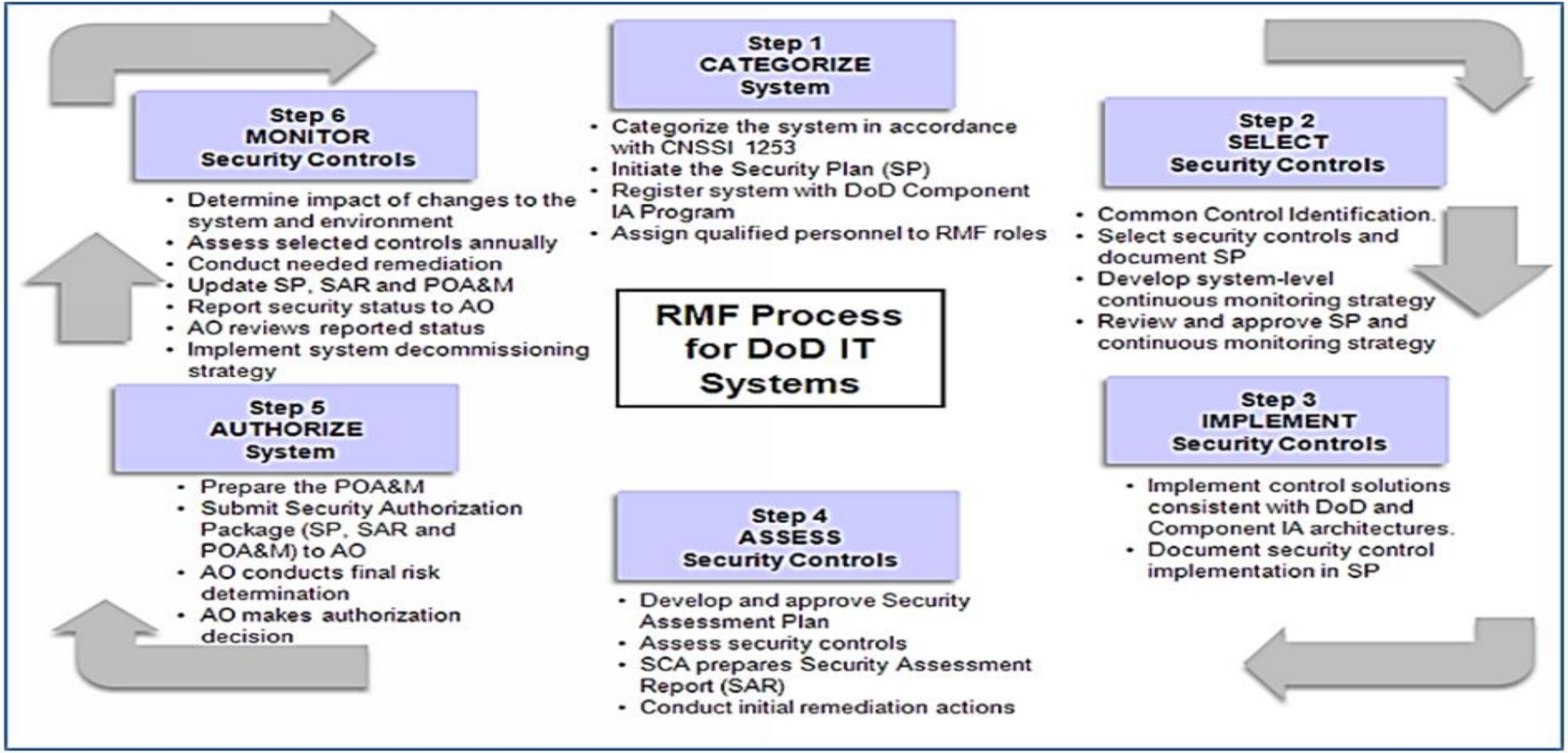
Grid authorities have issued a record $10 million fine to an unidentified utility over more than 120 security violations spanning four years.

Common Myths

- only applies if project started after RMF/UFC in effect
- only applies to systems connected to Internet
- only applies to systems connected to other network/systems
- only applies when contractor will supply new control systems or system components (modification of a system requires mitigation of cybersecurity risk during construction)

03 The How

Risk management framework (RMF)



RMF Process for DoD IT Systems

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

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

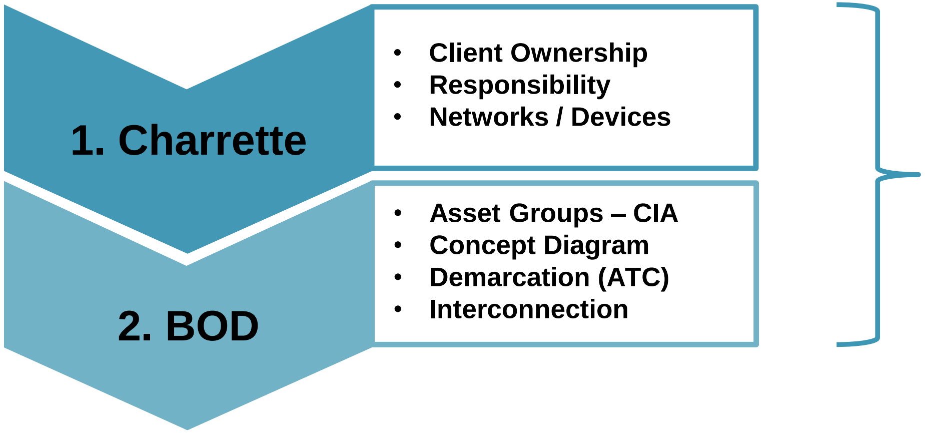
- Prepare the POA&M
- Submit Security Authorization Package (SP, SAR and POA&M) to AO
- AO conducts final risk determination
- AO makes authorization decision

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

UFC-4-010-06 CYBERSECURITY PLANNING / 1391 DEVELOPMENT

Cybersecurity Process Flow



1. Charrette

- **Client Ownership**
- **Responsibility**
- **Networks / Devices**

2. BOD

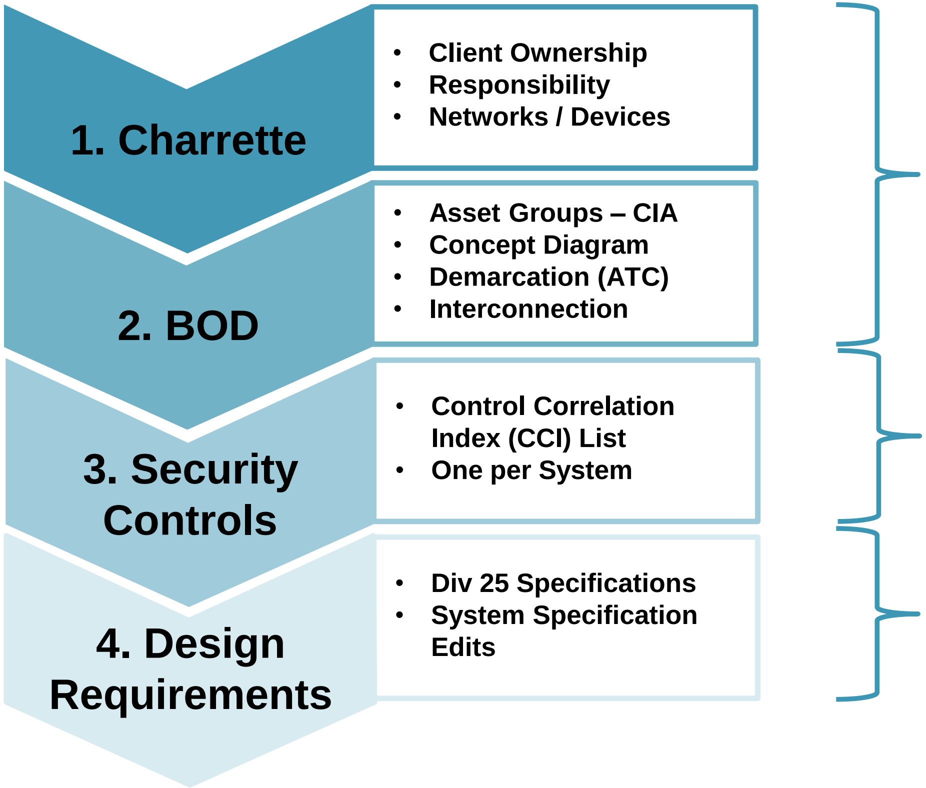
- **Asset Groups – CIA**
- **Concept Diagram**
- **Demarcation (ATC)**
- **Interconnection**

15% Design
Affects Cost Estimates

dd1391 must include cybersecurity costs and statement of work/UFC requirement

UFC-4-010-06 CYBERSECURITY DESIGN BID BUILD

Cybersecurity Process Flow



1. Charrette

- Client Ownership
- Responsibility
- Networks / Devices

2. BOD

- Asset Groups – CIA
- Concept Diagram
- Demarcation (ATC)
- Interconnection

3. Security Controls

- Control Correlation Index (CCI) List
- One per System

4. Design Requirements

- Div 25 Specifications
- System Specification Edits

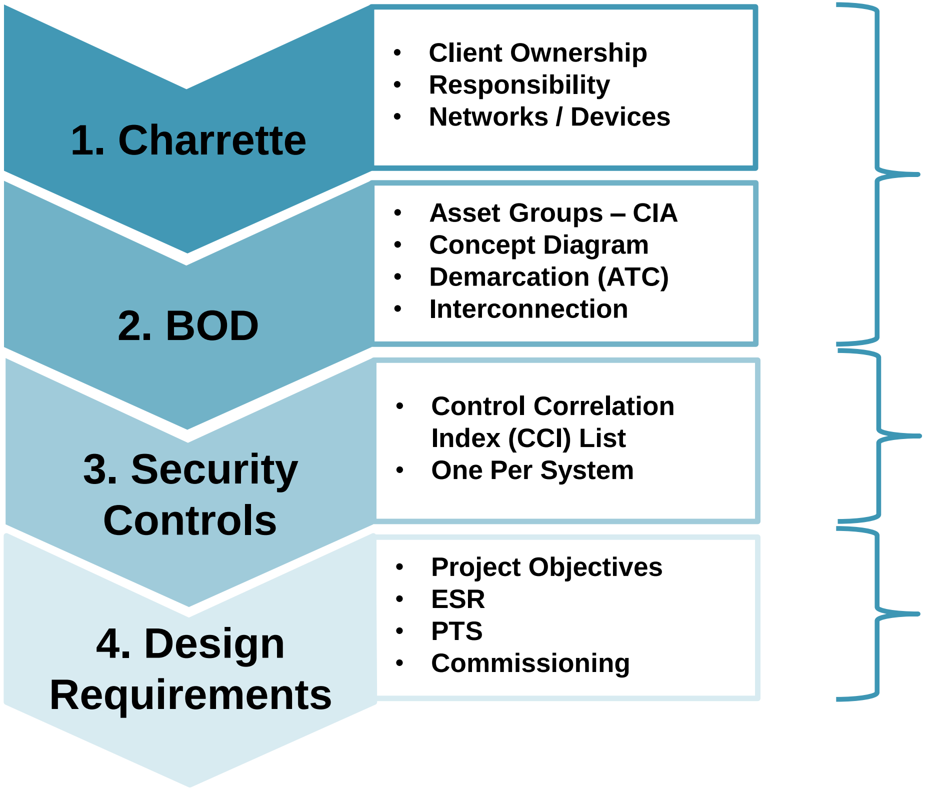
15% Design

30% Design

Follows normal design progression
UFGS:
25 05 11 (one per system)
25 08 10 (one per new front-end)
25 08 11.00 20 (NAVY Only)
25 10 10 (one per front-end)

UFC-4-010-06 CYBERSECURITY DESIGN BUILD RFP

Cybersecurity Process Flow



1. Charrette
   - Client Ownership
   - Responsibility
   - Networks / Devices

2. BOD
   - Asset Groups – CIA
   - Concept Diagram
   - Demarcation (ATC)
   - Interconnection

3. Security Controls
   - Control Correlation Index (CCI) List
   - One Per System

4. Design Requirements
   - Project Objectives
   - ESR
   - PTS
   - Commissioning

15% Design

Not provided in RFP – Require by AE2 in design requirements

Follows normal design progression

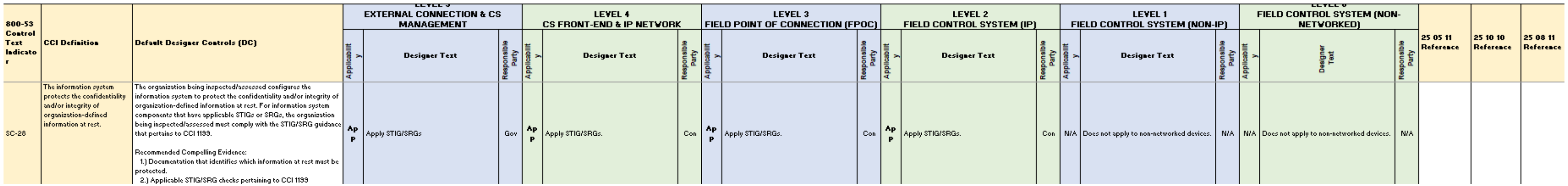
Facility Ratings & System Classifications

Facility Rating: MISSION SUPPORT				
Owner	**System Group**	**System**	**C-I-A**	**NOTES**
TBD	UMCS	Electrical Systems (ES)	L-L-L	
		HVAC & Subsystems		
		Building Lighting System (BLS)		
		Water Meters		
	UCS	EEDRS (Enterprise Energy Data Reporting System)	M-M-M	Gas & Electric Metering
		Generator & Battery System		
	BCS	Conveyance/Vertical Transport System (Elevators)	L-L-M	
	FLS	Fire Alarm Reporting System (FARS)	L-M-M	
		Fire Suppression System (FSS)		
		Mass Notification System (MNS)		
	ESS	Physical Access Control Systems (PACS)		Government Furnished
		Intrusion Detection System (IDS)		
		Video Monitoring Systems/Closed Circuit TV (CCTV)		

Security Controls (*CCI List*)

Analysis, Documentation, and Required Client Approval

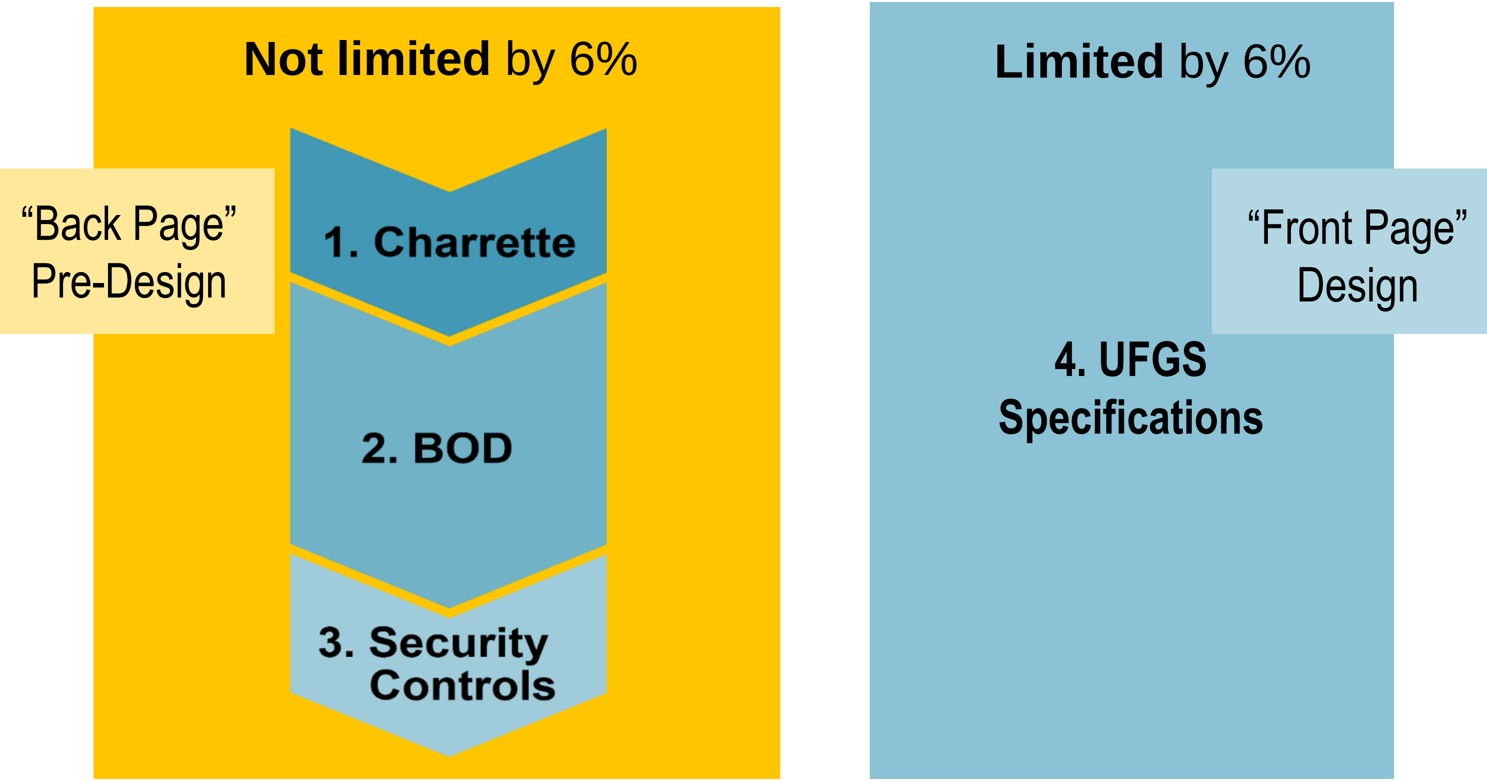
- Each CCI List (spreadsheet tab): 200-1400 rows X 6 Network Levels
- One CCI List per System Group (HVAC, FLS, BAS, etc.)
- At least two UFGS Specs per CCI List



800-53 Control Text Indicator	CCI Definition	Default Designer Controls (DC)	LEVEL 5 EXTERNAL CONNECTION & CS MANAGEMENT			LEVEL 4 CS FRONT-END & IP NETWORK			LEVEL 3 FIELD POINT OF CONNECTION (FPOC)			LEVEL 2 FIELD CONTROL SYSTEM (IP)			LEVEL 1 FIELD CONTROL SYSTEM (NON-IP)			LEVEL 0 FIELD CONTROL SYSTEM (NON-NETWORKED)			25 05 11 Reference	25 10 10 Reference	25 08 11 Reference
			Applicability	Designer Text	Responsible Party	Applicability	Designer Text	Responsible Party	Applicability	Designer Text	Responsible Party	Applicability	Designer Text	Responsible Party	Applicability	Designer Text	Responsible Party	Applicability	Designer Text	Responsible Party			
SC-28	The information system protects the confidentiality and/or integrity of organization-defined information at rest.	The organization being inspected/assessed configures the information system to protect the confidentiality and/or integrity of organization-defined information at rest. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1199. Recommended Compelling Evidence: 1.) Documentation that identifies which information at rest must be protected. 2.) Applicable STIG/SRG checks pertaining to CCI 1199	AP	Apply STIG/SRGs	Gov	AP	Apply STIG/SRGs.	Con	AP	Apply STIG/SRGs.	Con	AP	Apply STIG/SRGs.	Con	N/A	Does not apply to non-networked devices.	N/A	N/A	Does not apply to non-networked devices.	N/A			

04 Costs

Federal/DoD – 6% Fee Limitation



Not limited by 6%

“Back Page”
Pre-Design

1. Charrette

2. BOD

3. Security Controls

Limited by 6%

“Front Page”
Design

4. UFGS Specifications

Budget Guidance for Cybersecurity

NAVY

- Primary Facilities
  - $100k for projects under $5M
  - $250k for projects over $5M
- Supporting Facilities
  - $100k for ECC <$10M
  - 1% for $10M < ECC < $50M

ARMY

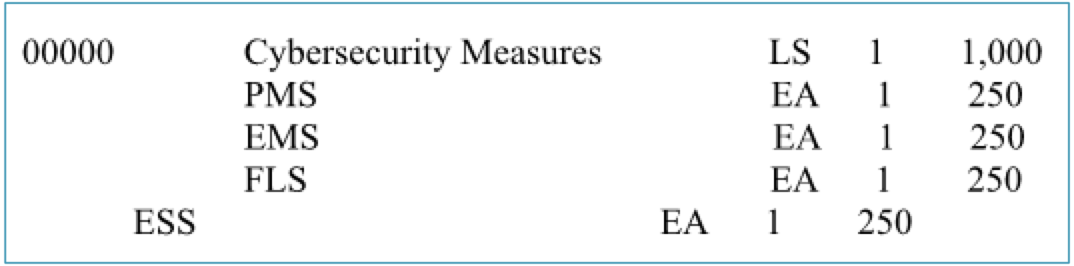
- $250k per Platform

AIR FORCE

- $250k Non-Mission Critical and <= 50,000 sq. ft
- 2.5% ECC Non-Mission Critical and >= 50,000 sq. ft

HDR Opinion of Probable Costs
(Sample CONUS Project Set)

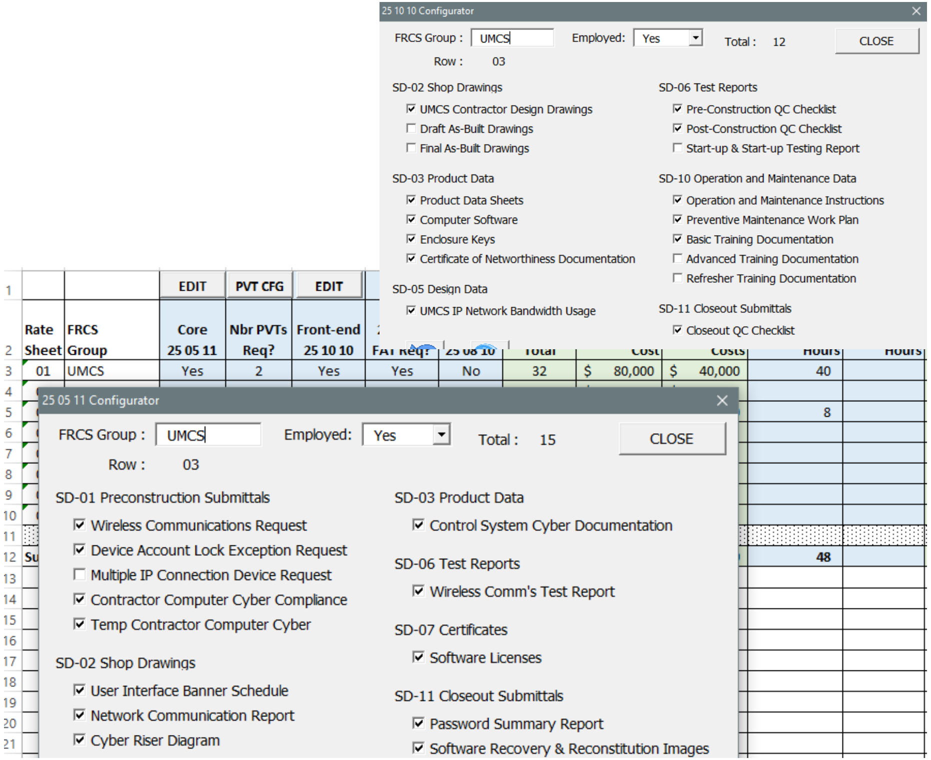
- Variable up to $500k
- Dependent on number of systems and front-end connectivity/scope



00000	Cybersecurity Measures	LS	1	1,000
	PMS	EA	1	250
	EMS	EA	1	250
	FLS	EA	1	250
	ESS	EA	1	250

Implementation Cost Impact (Contractor Costs)

- **Direct Impacts:**
  - 25 05 11
    - Up to 23 Submittals (18 core)
    - Up to 3 PVTs
    - Cyber Support Hours
  - 25 10 10
    - Up to 16 Submittals
    - Up to 3 PVTs
  - 25 08 10
    - Up to 4 Submittals
    - Off-site Factory Test
    - Documented Test Plans



25 10 10 Configurator

FRCS Group : UMCS Employed: Yes Total : 12 CLOSE

Row : 03

SD-02 Shop Drawings
- ☑ UMCS Contractor Design Drawings
- □ Draft As-Built Drawings
- □ Final As-Built Drawings

SD-03 Product Data
- ☑ Product Data Sheets
- ☑ Computer Software
- ☑ Enclosure Keys
- ☑ Certificate of Networthiness Documentation

SD-05 Design Data
- ☑ UMCS IP Network Bandwidth Usage

SD-06 Test Reports
- ☑ Pre-Construction QC Checklist
- ☑ Post-Construction QC Checklist
- □ Start-up & Start-up Testing Report

SD-10 Operation and Maintenance Data
- ☑ Operation and Maintenance Instructions
- ☑ Preventive Maintenance Work Plan
- ☑ Basic Training Documentation
- □ Advanced Training Documentation
- □ Refresher Training Documentation

SD-11 Closeout Submittals
- ☑ Closeout QC Checklist

			EDIT	PVT CFG	EDIT							
2	Rate Sheet	FRCS Group	Core 25 05 11	Nbr PVTs Req?	Front-end 25 10 10	FAT Req?	25 08 10	Total	Cost	Costs	Hours	Hours
3	01	UMCS	Yes	2	Yes	Yes	No	32	$ 80,000	$ 40,000	40	
5											8	
12	Su										48	

25 05 11 Configurator

FRCS Group : UMCS Employed: Yes Total : 15 CLOSE

Row : 03

SD-01 Preconstruction Submittals
- ☑ Wireless Communications Request
- ☑ Device Account Lock Exception Request
- □ Multiple IP Connection Device Request
- ☑ Contractor Computer Cyber Compliance
- ☑ Temp Contractor Computer Cyber

SD-02 Shop Drawings
- ☑ User Interface Banner Schedule
- ☑ Network Communication Report
- ☑ Cyber Riser Diagram

SD-03 Product Data
- ☑ Control System Cyber Documentation

SD-06 Test Reports
- ☑ Wireless Comm's Test Report

SD-07 Certificates
- ☑ Software Licenses

SD-11 Closeout Submittals
- ☑ Password Summary Report
- ☑ Software Recovery & Reconstitution Images

05 Q&A