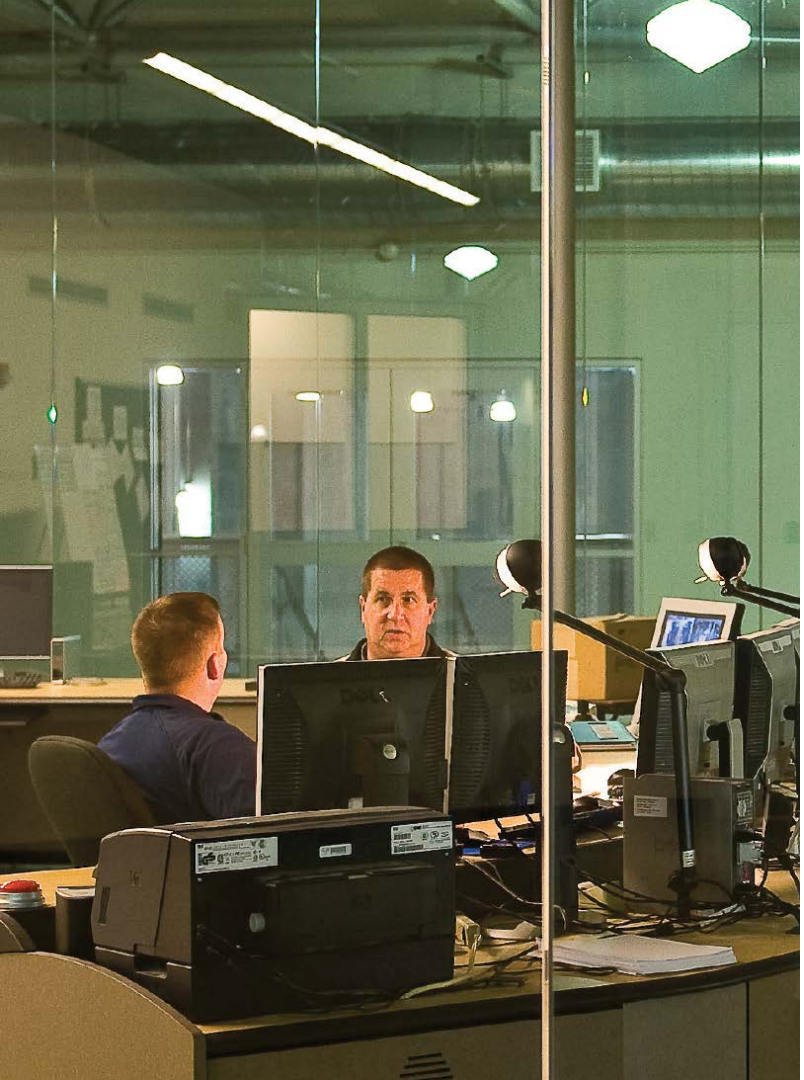
# UFC-4-010-06 Requirements Overview

August 17, 2020

# Presenter

David Brearley, GISCP, PMP
Program Manager, Cybersecurity
*David.Brearley@hdrinc.com*



# AGENDA

01 The Why

02 The What

03 The How

04 Costs

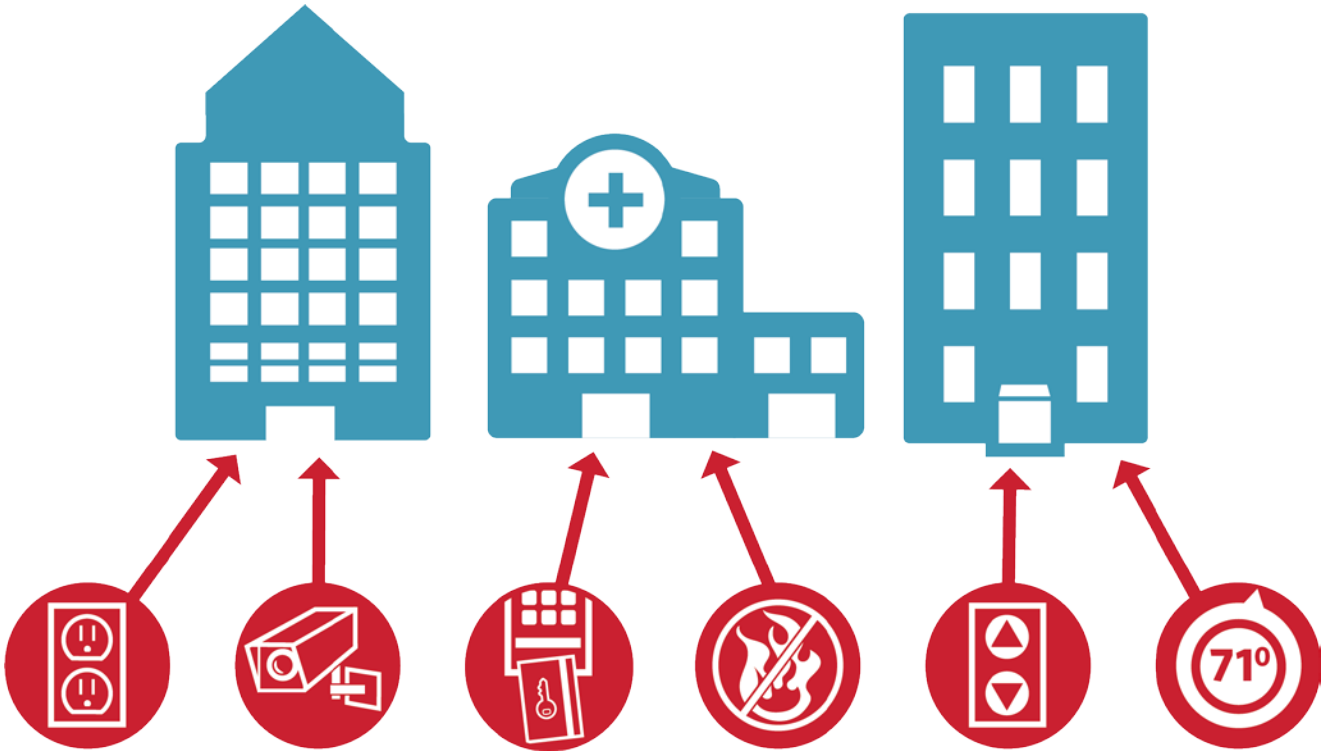
05 Q&A

# 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

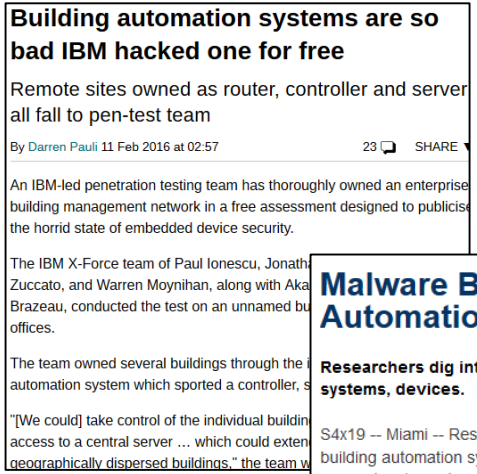
# Cybersecurity Threats to Critical Infrastructure



# Cybersecurity Threats to Energy/Power

# Cybersecurity Threats to Energy/Power

# Cybersecurity Threats to Critical Infrastructure



**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

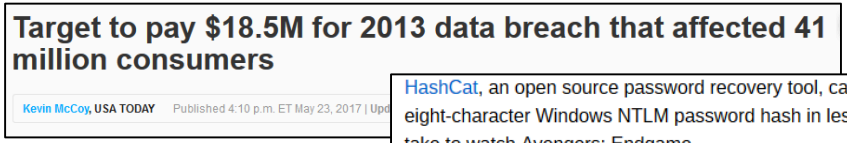
By Darren Pauli 11 Feb 2016 at 02:57 23 SHARE

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 | Upd

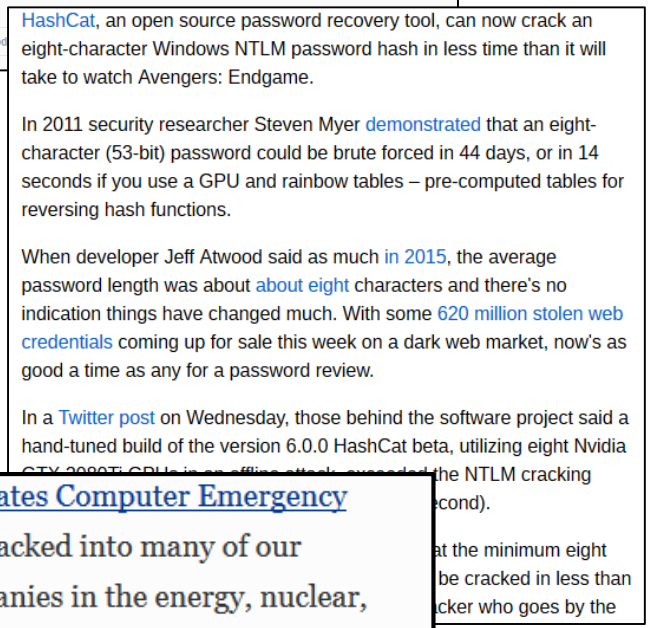
**Malware Built to Hack Building Automation Systems**

**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



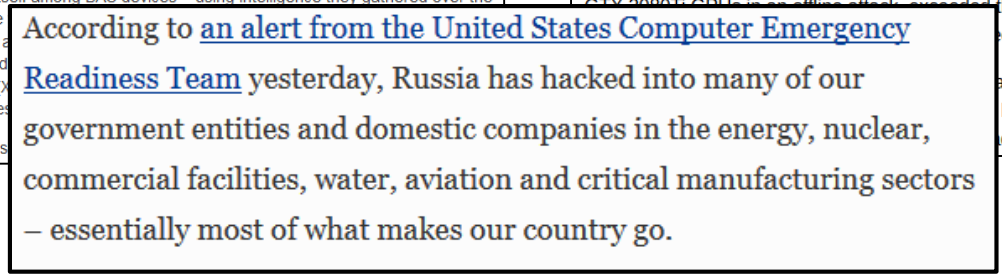
HashCat, an open source password recovery tool, can now crack an eight-character Windows NTLM password hash in less time than it will take to watch Avengers: Endgame.

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 hand-tuned build of the version 6.0.0 HashCat beta, utilizing eight Nvidia GTX 2080Ti GPUs in an offline attack, exceeded the NTLM cracking econd).

at the minimum eight be cracked in less than acker who goes by the

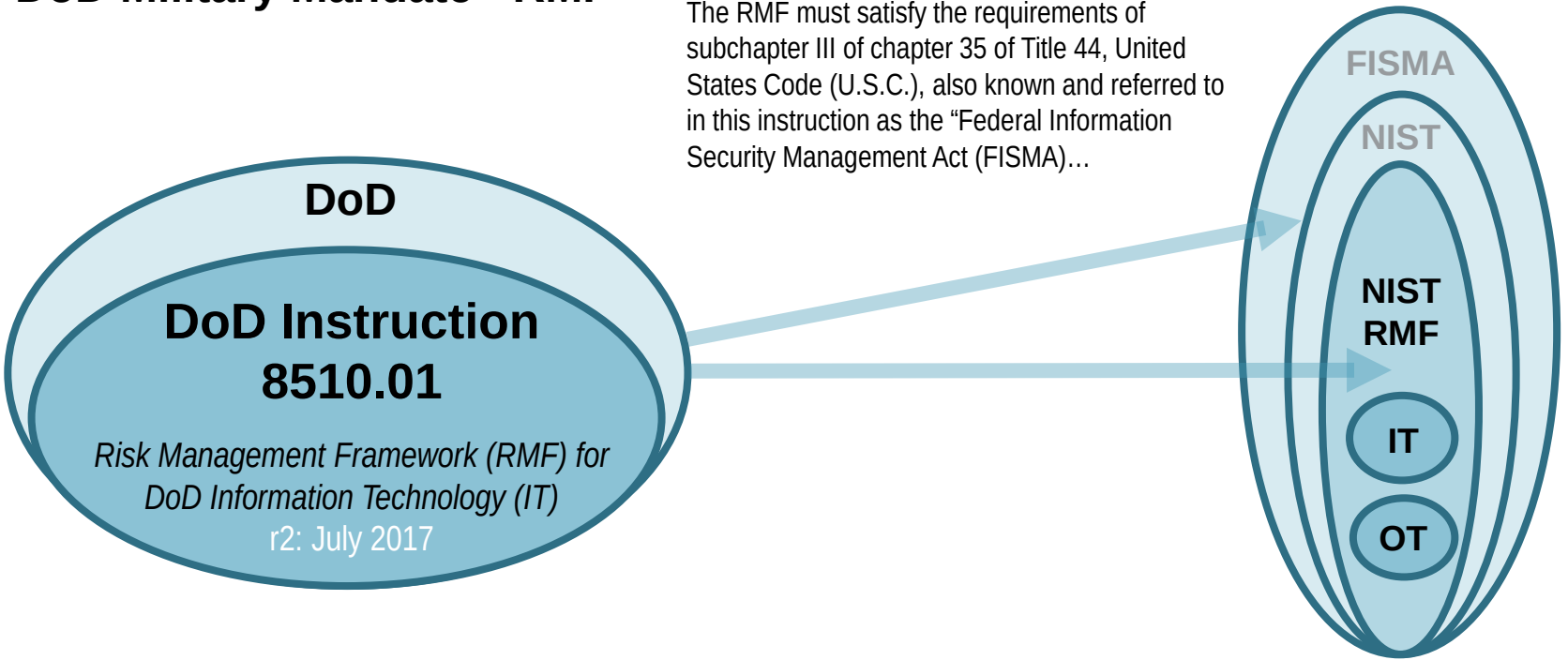


According to an alert from the United States Computer Emergency Readiness Team yesterday, Russia has hacked into many of our government entities and domestic companies in the energy, nuclear, commercial facilities, water, aviation and critical manufacturing sectors – essentially most of what makes our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

# 02 The What

# DoD Military Mandate - RMF

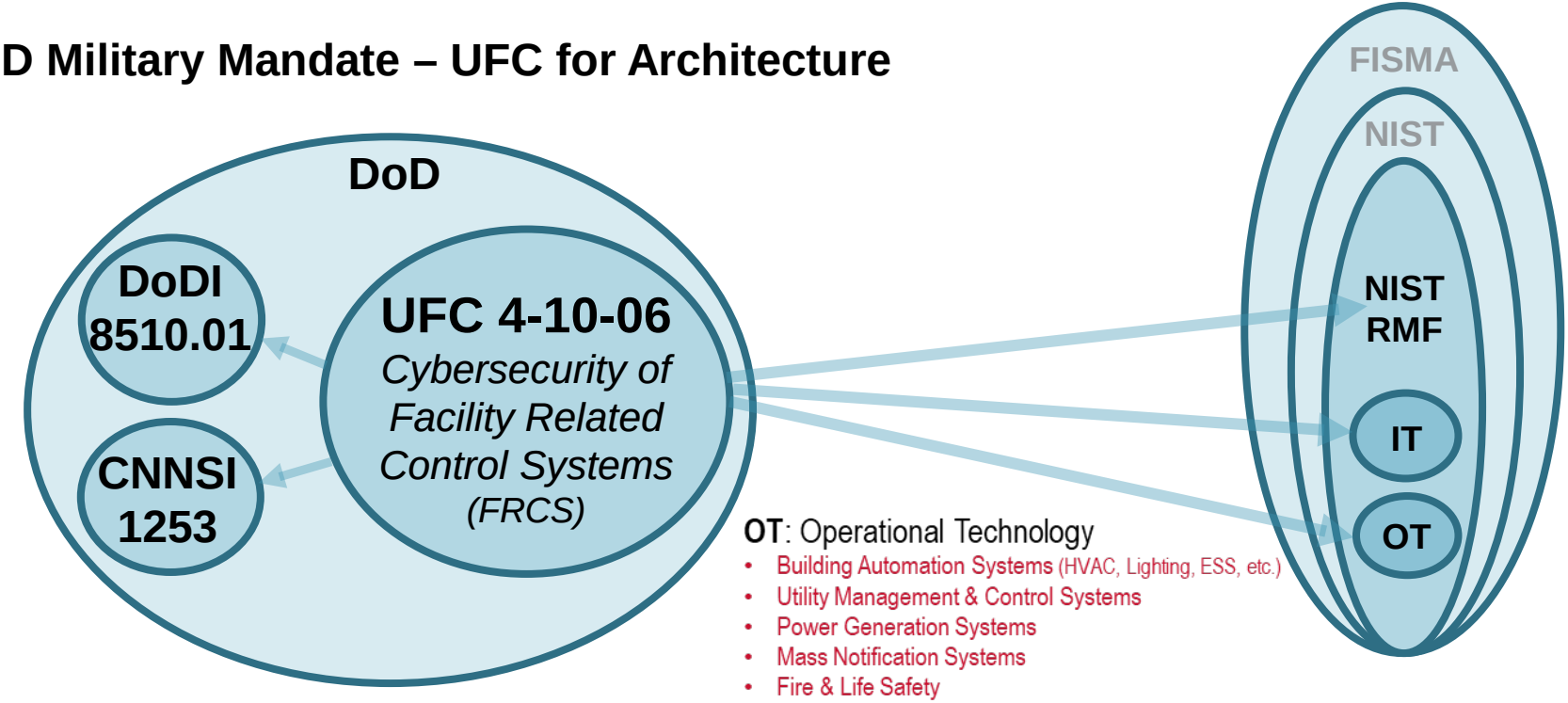
The RMF must satisfy the requirements of subchapter III of chapter 35 of Title 44, United States Code (U.S.C.), also known and referred to in this instruction as the “Federal Information Security Management Act (FISMA)…




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




**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

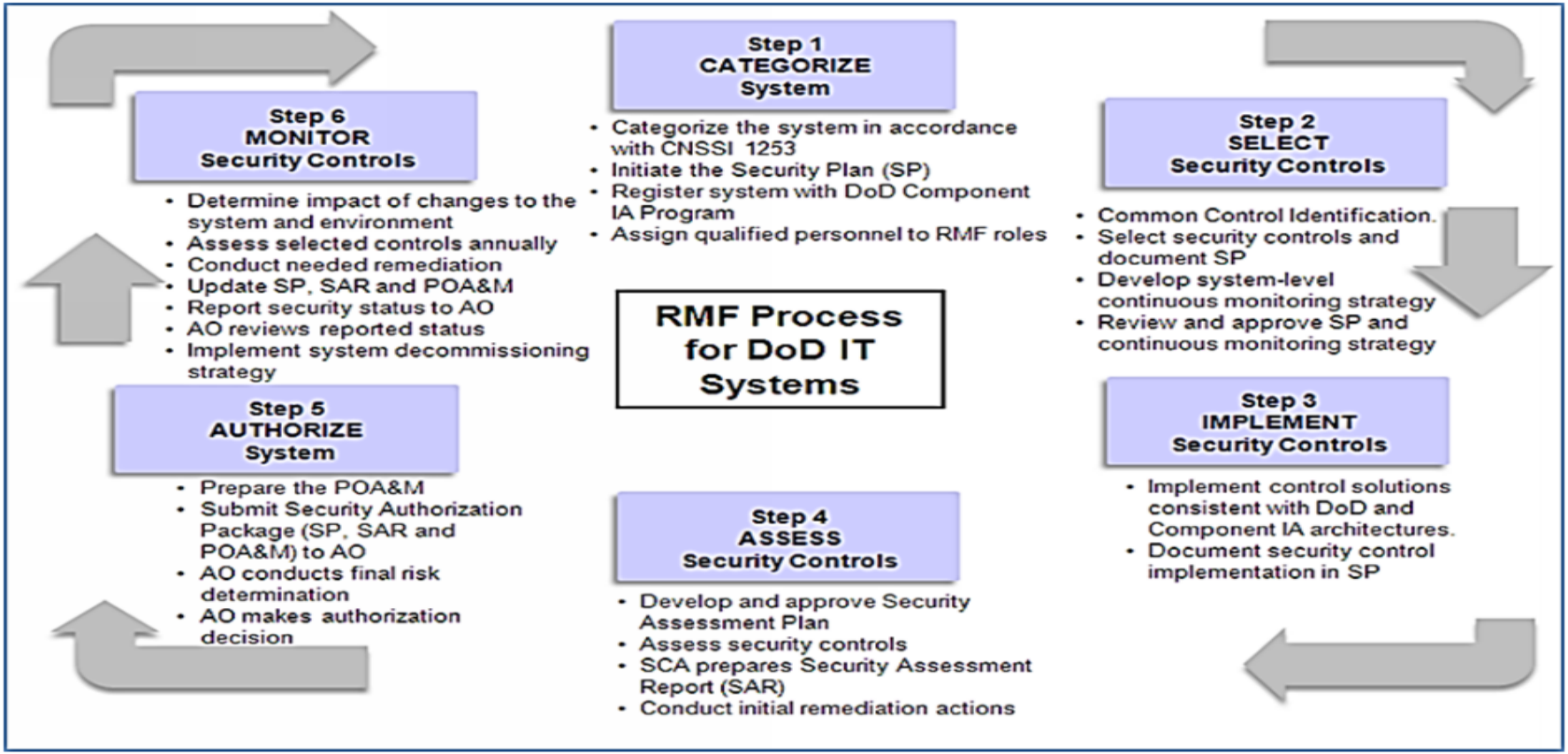
Grid authorities have issued a record $10 million fine to an unidentified utility over more than 120 security violations spanning four years.

## 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)

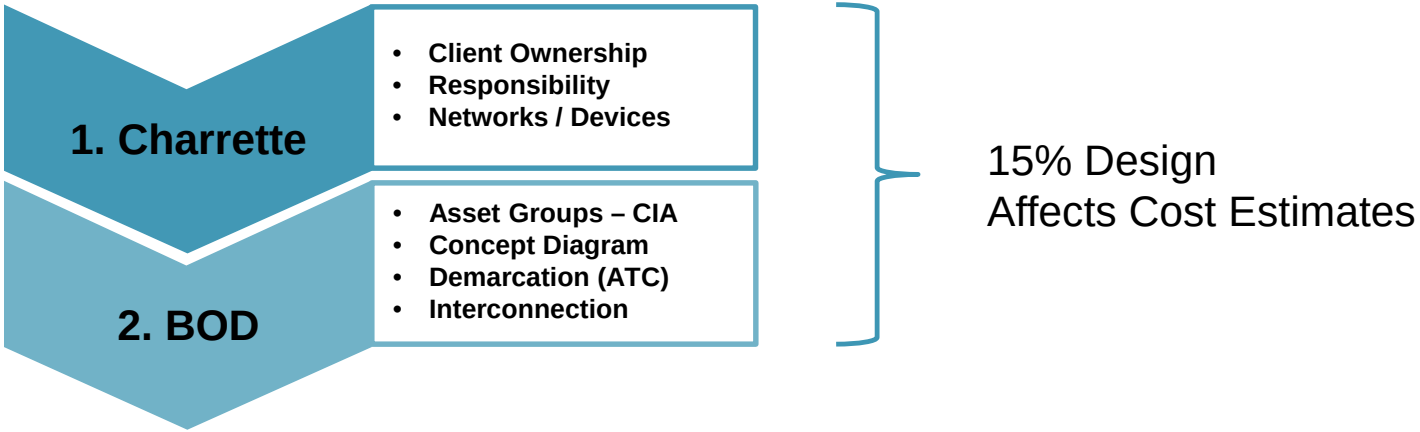
# 03 The How

# Risk management framework (RMF)



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

Cybersecurity Process Flow

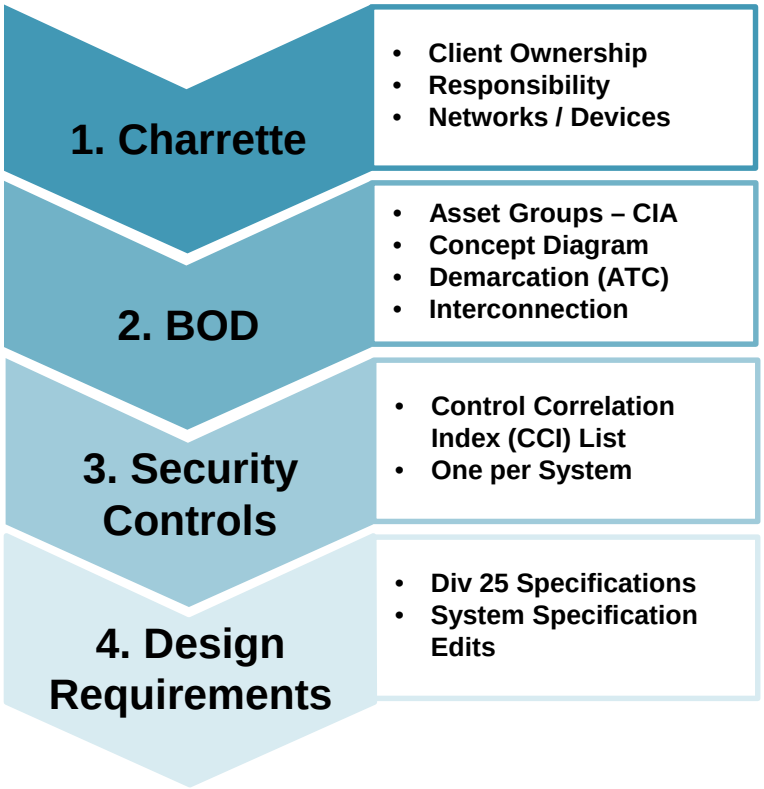



15% Design
Affects Cost Estimates

*DD1391 must include cybersecurity costs and statement of work/UFC requirement

# UFC-4-010-06 CYBERSECURITY DESIGN BID BUILD

## Cybersecurity Process Flow



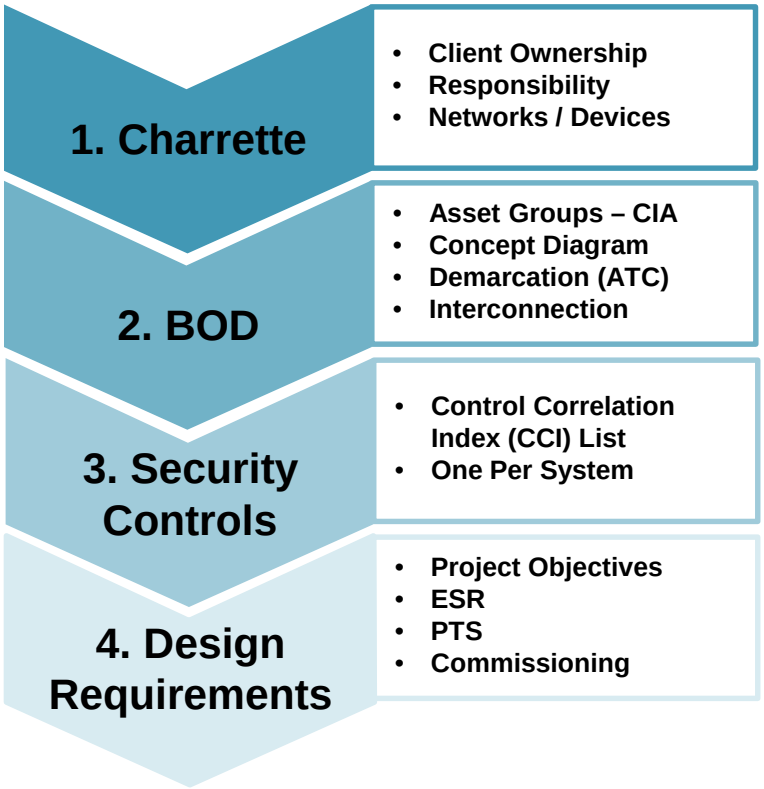

15% Design

30% Design

Follows normal design progression
UFGS:
25 05 11 (one per system)
25 10 10 (one per front-end)

# UFC-4-010-06 CYBERSECURITY DESIGN BUILD RFP

## Cybersecurity Process Flow




15% Design

Not provided in RFP – Require by AE2 in design requirements

Follows normal design progression

# 04 Costs

# Federal/DoD – 6% Fee Limitation

# 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 | |

# 05 Q&A