The PMC Group LLC

*Engineering a better tomorrow today*

# SAME Webinar

# National Critical Infrastructure and Resilience Month Presentation

# Cybersecurity of Facility-Related Control Systems (FRCS) and the DoD CIO Risk Management Framework


## Michael Chipley PhD GICSP PMP LEED AP

**Cyber SME Supporting Principal Cyber Advisor, Energy and ESCTP Offices**


Society of SAME American Military Engineers

## November 14, 2019

# FRCS Cyber and DFARS 254.204-7012

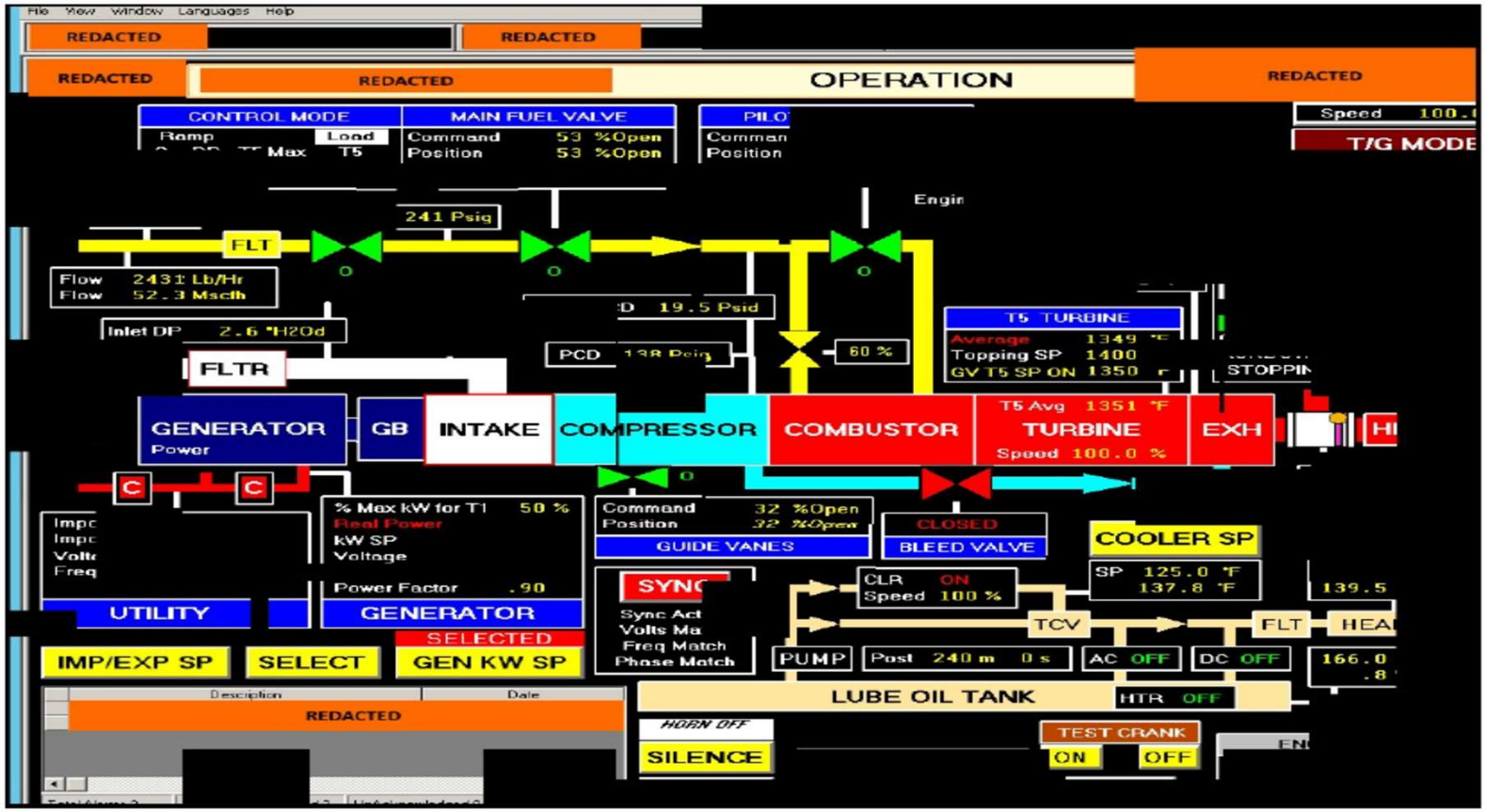
**Todays Topics**

**Cybersecuring Facility-Related Control Systems:** Using the NIST SP 800-82 Securing Industrial Control Systems Security Guide, the Cybersecuring FRCS Unified Facility Criteria (UFC) and Unified Facility Guide Specifications (UFGS), creating the Test and Development Environment (TDE), and Facility Security Operations Centers, new Contract Language, DoD ACI TTP's

**DFARS 254.204-7012:** - **ALL** contractors/vendors doing business with the DoD must have a NIST SP 800-171 compliant Cyber Risk Management Plan (CRMP) for their business systems that have Controlled Unclassified Information (CUI) and will initially self-attest, and as of Jan 2019 the Defense Contract Management Agency is responsible for ensuring contractor compliance

# US-CERT Alert TA18-074A Energy System Attack

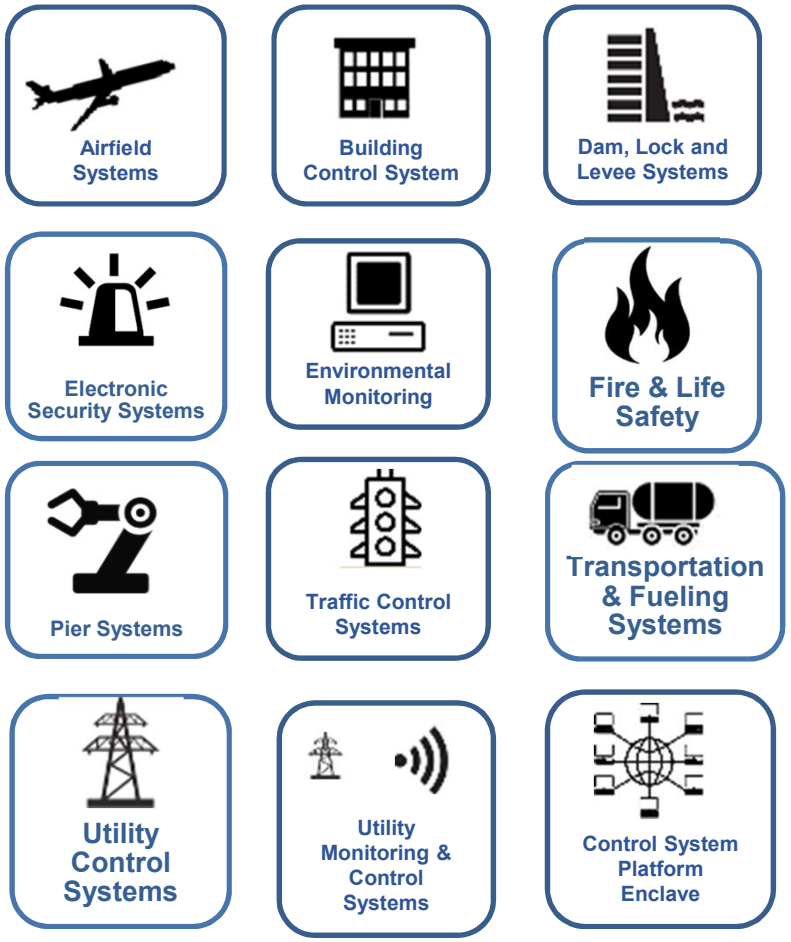
Russian Government Targeting Energy and Critical Infrastructure
March 2018 - Compromised control system screenshot below




https://www.us-cert.gov/ncas/alerts/TA18-074A

# DoD Facility Related Control Systems (FRCS)

## Categories

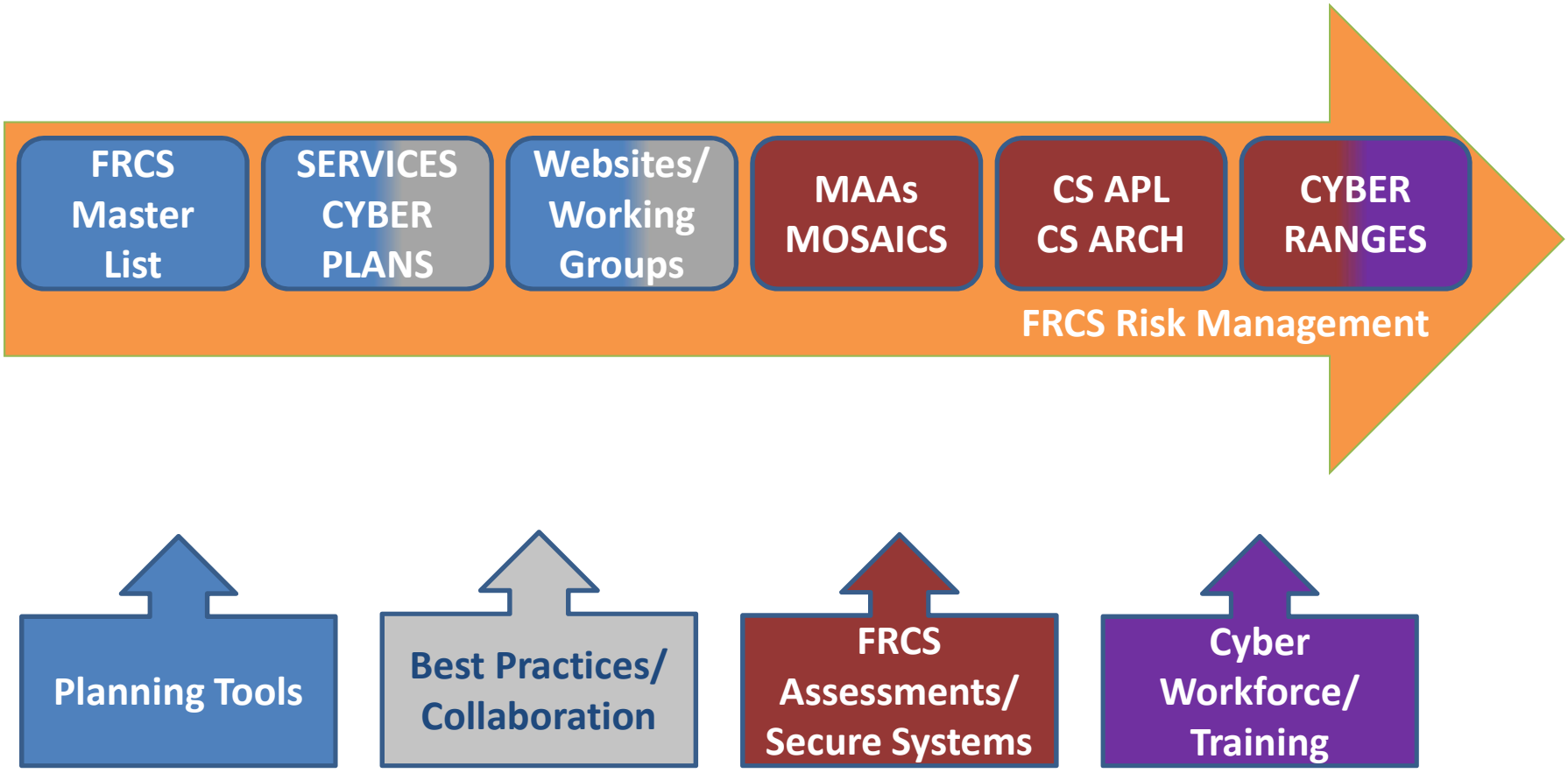



## Systems

- Building Automation System
- Building Lighting System
- Conveyance/Vertical Transport System
- Electrical Systems
- Heating, Ventilation, Air Conditioning
- Irrigation System
- Shade Control System
- Vehicle Charging System
- Cathodic Protection Systems
- Compressed Air (Or Compressed Gases) System
- Central Plant (District) Chilled Water System
- Central Plant (District) Electrical Power Production
- Central Plant (District) Hot Water System
- Central Plant (District) Steam System
- Electrical Distribution System
- Gray Water System
- Industrial Waste Treatment System
- Microgrid Control Systems
- Natural Gas System
- Oily Water/Waste Oil System
- Potable Water System
- Pure Water System
- Salt Water System
- Sanitary Sewer/Wastewater System
- Utility Metering System (Advanced Meters, AMI, etc.)
- *Many More…*

**DoD Control Systems are just as vulnerable as industry, how do we protect them?**

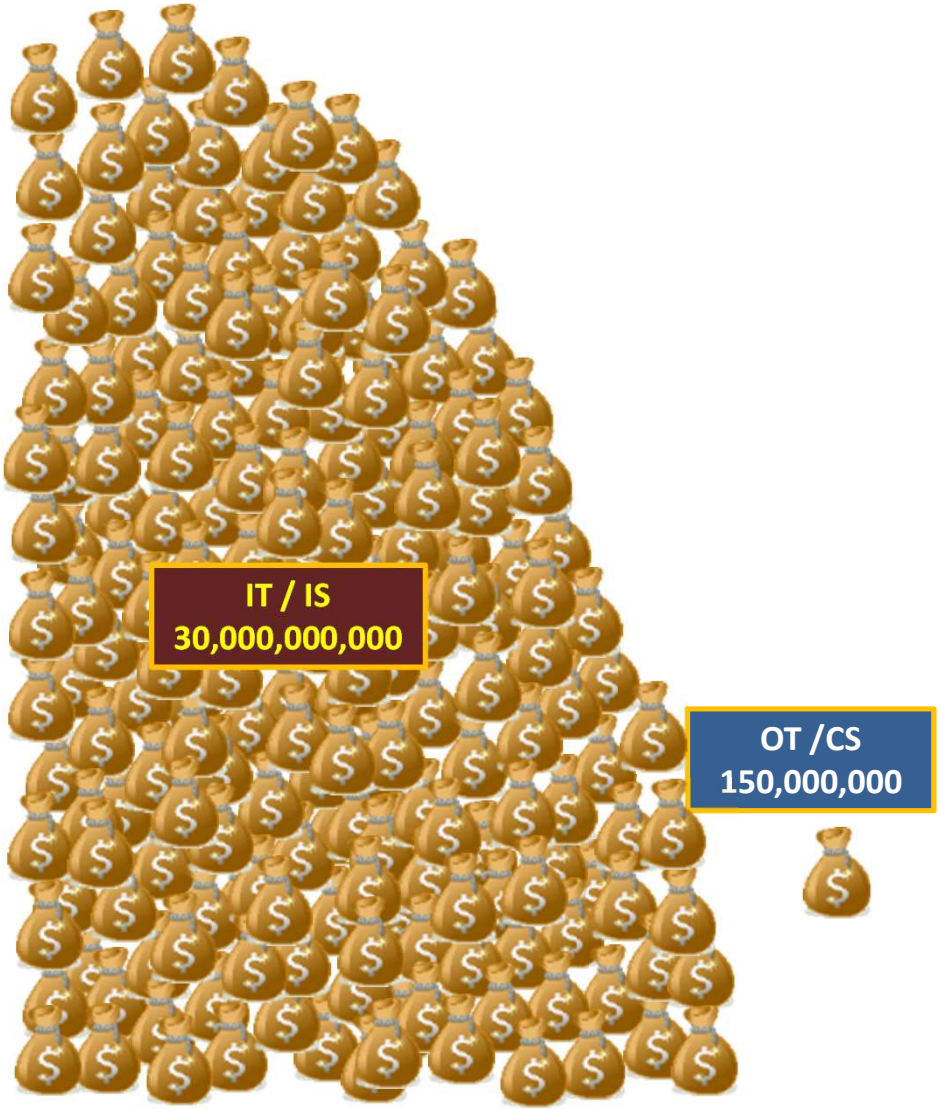
# ODASD(E) Cybersecurity Initiatives



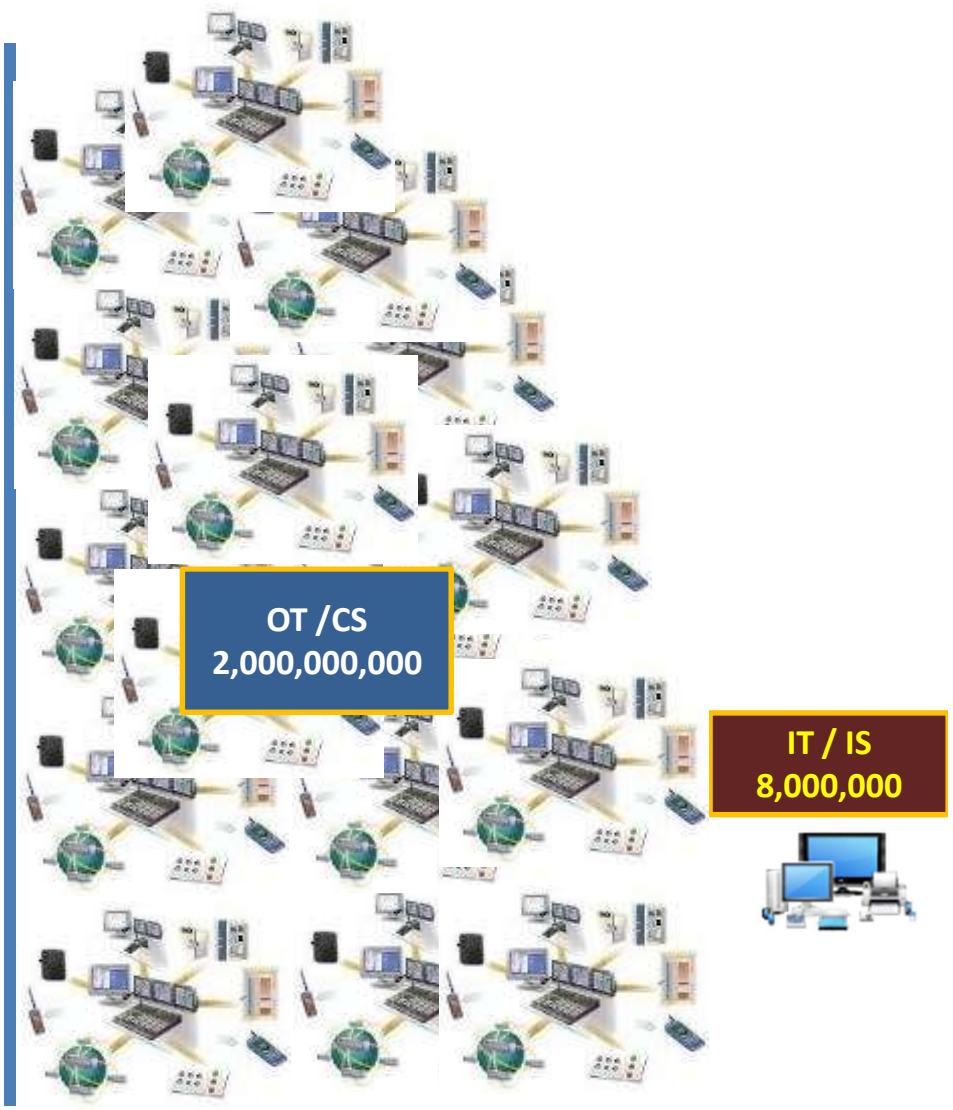

***Alignment with Federal, Industry Objectives***

# IT/IS Versus OT/CS Budgets and Devices

## *DoD Budget $M*




## *DoD # of Devices*



# Operational Technology and FRCS


https://serdp-estcp.org/Tools-and-Training/Installation-Energy-and-Water/Cybersecurity

# Standards – NIST SP 800-82 R2


This document provides guidance for establishing secure industrial control systems (ICS). These ICS, which include supervisory control and data acquisition (SCADA) systems, distributed control systems (DFRCS), and other control system configurations such as skid-mounted Programmable Logic Controllers (PLC) are often found in the industrial control sectors.

**This document provides an overview of these ICS and typical system topologies, identifies typical threats and vulnerabilities to these systems, and provides recommended security countermeasures to mitigate the associated risks.**

800-82 Rev 2 was released May 2015 – has 800-53 Rev 4 800+ controls,
**Appendix G ICS Overlay**

# NIST SP 800-82 R2 Key Security Controls

### Inventory
- CM-8 Information System Component Inventory
- PM-5 Information System Inventory
- PL-7 Security Concept of Operations
- PL-8 Information Security Architecture
- SC-41 Port and I/O Device Access
- PM-5 Information System Inventory

### Central Monitoring
- AU-6 Audit Review, Analysis, and Reporting
- CA -7 Continuous Monitoring
- IR-5 Incident Monitoring
- IR-6 Incident Reporting
- PE-6 Monitoring Physical Access
- PM-14 Testing, Training and Monitoring
- RA-5 Vulnerability Scanning
- SC-7 Boundary Protection
- SI-4 Information System Monitoring
- SI-5 Security Alerts, Advisories, and Directives

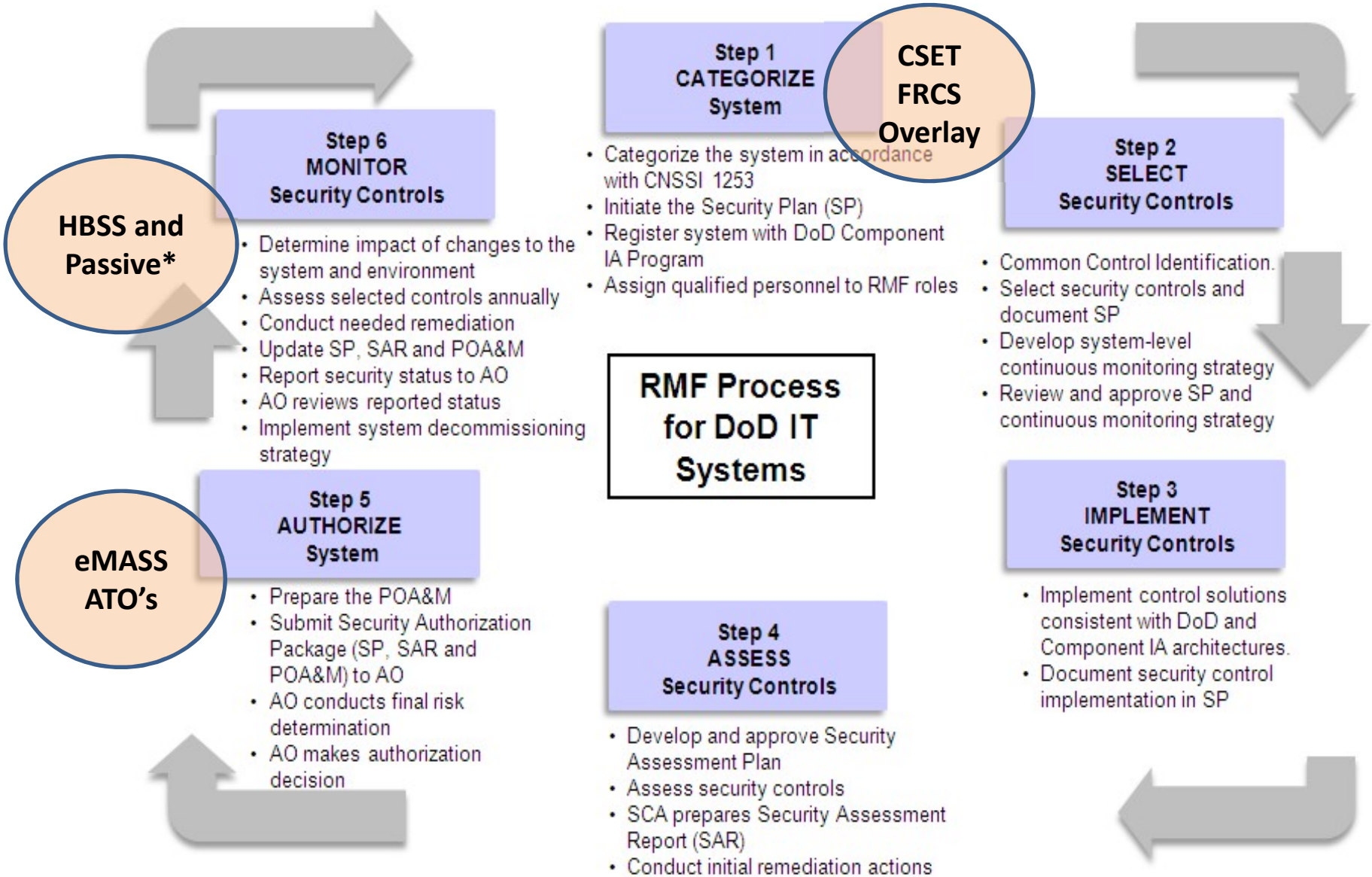
### Test and Development Environment
- CA-8 Penetration Testing
- CM-4 Security Impact Analysis
- CP-3 Contingency Training
- CP-4 Contingency Plan Testing and Exercises
- PM-14 Testing, Training and Monitoring

### Critical Infrastructure
- CP-2 Contingency Plan
- CP-6 Alternate Storage Site
- CP-7 Alternate Processing Site
- CP-10 Information System Recovery and Reconstitution
- PE-3 Physical Access Control
- PE-10 Emergency Shutoff
- PE-11 Emergency Power
- PE-12 Emergency Lighting
- PE-13 Fire Protection
- PE-14 Temperature and Humidity Controls
- PE-17 Alternate Work Site
- PM-8 Critical Infrastructure Plan

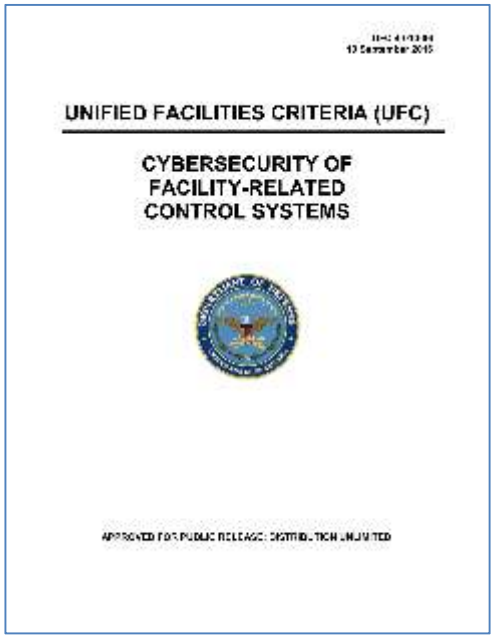
### Acquisition and Contracts
- AU-6 Audit Review, Analysis, and Reporting
- CA -7 Continuous Monitoring
- SA-4 Acquisitions
- PM-3 Information System Resources
- PM-14 Testing, Training and Monitoring

**Inbound Protection, Outbound Detection**

# FRCS Overlay & RMF Implementation



# DoD UFC 4-010-06 Cybersecurity


UNIFIED FACILITIES CRITERIA (UFC)

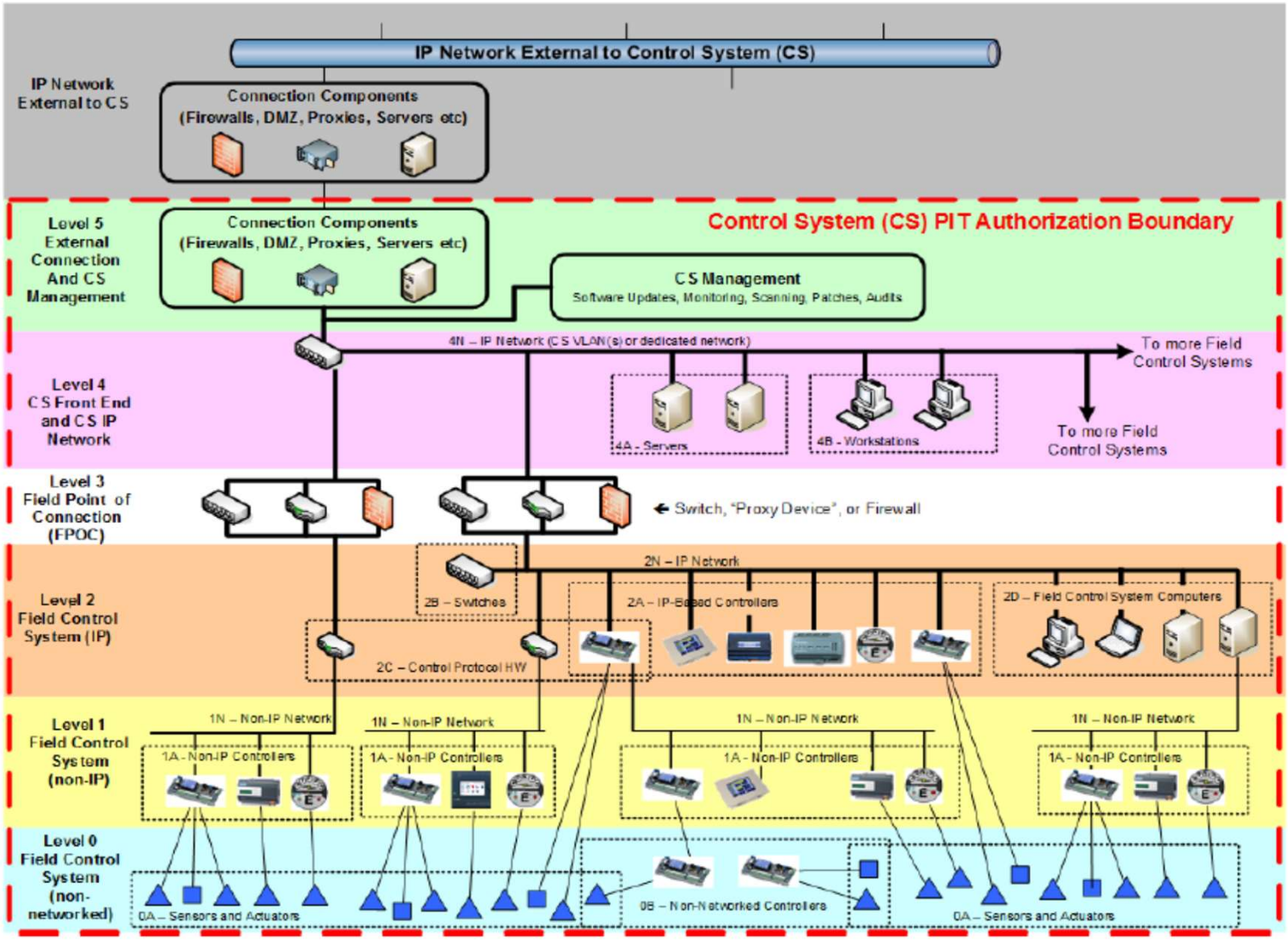
CYBERSECURITY OF FACILITY-RELATED CONTROL SYSTEMS

**3-1.1 Five Steps for Cybersecurity Design.** The five steps for cybersecurity design are:

**Step 1:** Based on the organizational mission and details of the control system, the System Owner (SO) and Authorizing Official (AO) **determine the Confidentiality, Integrity, and Availability** (C-I-A) impact levels (LOW, MODERATE, or HIGH) for the control system.
**Step 2:** Use the impact levels to select the proper list of controls from NIST SP 800-82.
**Step 3:** Using the DoD master Control Correlation Identifier (CCI) list, **create a list of relevant CCIs** based on the controls selected in Step 2.
**Step 4:** Categorize CCIs and identify CCIs that require input from the designer or are the designer's responsibility.
**Step 5**: Include cybersecurity requirements in the project specifications and provide input to others as required.

# UFC Reference Architecture

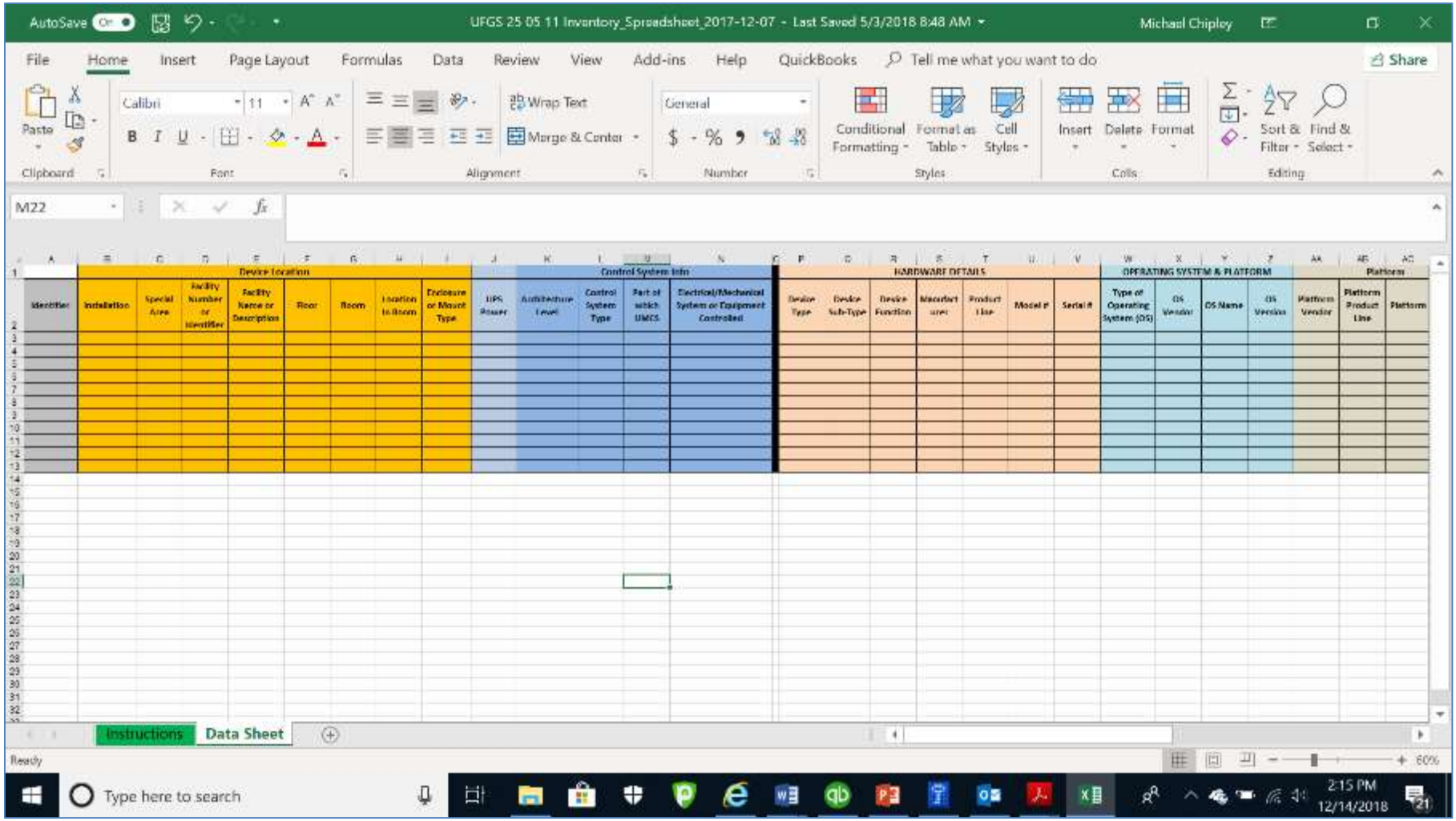
**Figure 2-1 5-Level Control System Architecture**



# UFGS 25 05 11 Cybersecurity For FRCS

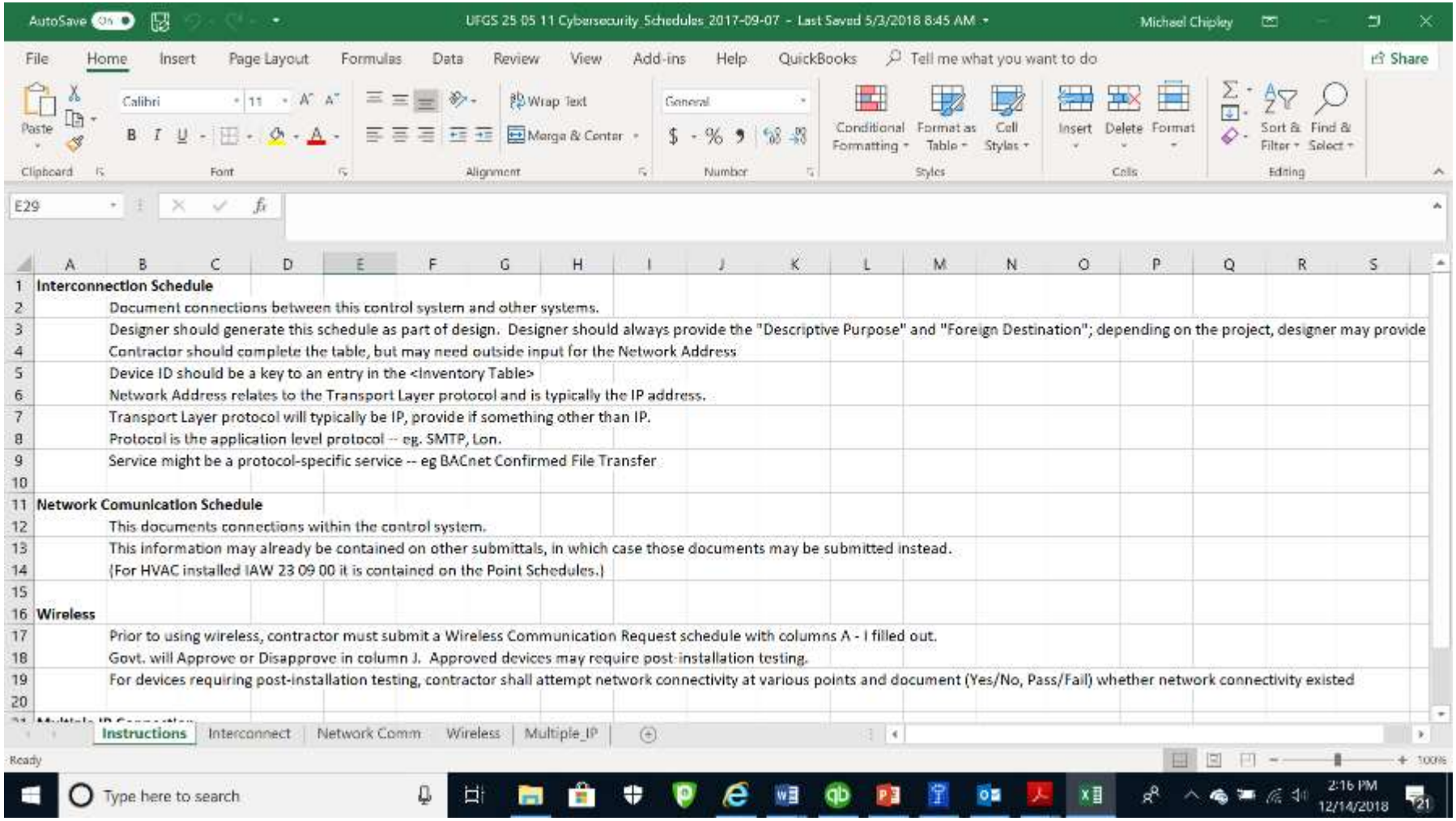

http://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-25-05-11

# UFGS 25 05 11 Inventory




http://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-25-05-11

# UFGS 25 05 11 Schedules



| | A | B |
|---|---|---|
| 1 | **Interconnection Schedule** | |
| 2 | | Document connections between this control system and other systems. |
| 3 | | Designer should generate this schedule as part of design. Designer should always provide the "Descriptive Purpose" and "Foreign Destination"; depending on the project, designer may provide |
| 4 | | Contractor should complete the table, but may need outside input for the Network Address |
| 5 | | Device ID should be a key to an entry in the <Inventory Table> |
| 6 | | Network Address relates to the Transport Layer protocol and is typically the IP address. |
| 7 | | Transport Layer protocol will typically be IP, provide if something other than IP. |
| 8 | | Protocol is the application level protocol -- eg. SMTP, Lon. |
| 9 | | Service might be a protocol-specific service -- eg BACnet Confirmed File Transfer |
| 10 | | |
| 11 | **Network Comunication Schedule** | |
| 12 | | This documents connections within the control system. |
| 13 | | This information may already be contained on other submittals, in which case those documents may be submitted instead. |
| 14 | | (For HVAC installed IAW 23 09 00 it is contained on the Point Schedules.) |
| 15 | | |
| 16 | **Wireless** | |
| 17 | | Prior to using wireless, contractor must submit a Wireless Communication Request schedule with columns A - I filled out. |
| 18 | | Govt. will Approve or Disapprove in column J. Approved devices may require post-installation testing. |
| 19 | | For devices requiring post-installation testing, contractor shall attempt network connectivity at various points and document (Yes/No, Pass/Fail) whether network connectivity existed |
| 20 | | |

http://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-25-05-11

# Create the Cyber Narrative



## Cybersecurity

### Cybersecurity Requirements

CODES AND REFERENCES

Facility-related controls systems will be designed in accordance with the following policies, standards and procedures:

- CNSSI 1253, Security Categorization And Control Selection For National Security Systems 2014
- CYBERCOM Advanced Industrial Control Systems Tactics, Techniques and Procedures, February 2017
- Department of Defense Instruction 8500.01, Cybersecurity, March 2014
- Department of Defense Instruction 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT), March 2014
- Department of Defense Instruction 8140 Cyberspace Workforce Management
- Department of Defense Instruction 8530 Cybersecurity Activities Support to DoD Information Network Operations March 2016
- Department of Defense Handbook for Self-Assessing Security Vulnerabilities & Risks of Industrial Control Systems on DoD Installations 2012
- Federal Information Processing Standard 200 Minimum Security Requirements for Federal Information and Information Systems
- Federal Information Processing Standard 201-2 Personal Identity Verification (PIV) of Federal Employees and Contractors
- Intelligence Community Directive (ICD) 706
- National Institute of Standards and Technology Special Publication 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems, February 2010
- National Institute of Standards and Technology Special Publication 800-53 R4 Security and Privacy Controls for Federal Information Systems and Organizations 2013
- National Institute of Standards and Technology Special Publication 800-82 R2 Guide to Industrial Control Systems (ICS) Security 2015
- National Institute of Standards and Technology Special Publication SP 800-115 Technical Guide to Information Security Testing and Assessment 2008
- UFC 3-410-01 Utility Monitoring And Control System (CS) Front End And Integration 2016
- UFC 3-410-02 Direct Digital Control For HVAC And Other Building Control Systems 2016
- UFC 4-010-06 Cybersecurity of Facility Related Control Systems, Change 1, 18 January 2017
- UFGS 23 09 00 Instrumentation and Control for HVAC
- UFGS 23 09 23.01 LonWorks® Direct Digital Control for HVAC and Other Building Systems



FACILITY-RELATED CONTROL SYSTEMS

The Integrated Facility Management Systems (IFMS), and all control systems including related communications networks and components, are considered Platform Information Technology (PIT). Design and provide all control systems in accordance with UFC 4-010-06 "Cybersecurity of Facility-Related Control Systems," National Institute of Standards and Technology (NIST), and Committee on National Security Systems (CNSS) documents.

The PROJECT cyber design needs to include, but is not limited to, the following FRCS:

- Electronic Security Systems – Owned and operated by security services
  - Electronic Emissions Detection Systems
  - Electronic Security System (ESS)[Bundled]
  - Digital Way-finding Signage Systems
  - Physical Access Control Systems (PACS)
  - Radio Frequency Detection Systems
  - Surveillance/Assessment Systems
  - Vehicle Access Barrier System
  - Active Shooter
  - CBRNE Notification Systems (CBRNE)
- Building Control Systems (BCS) - Owned and operated by Facilities
  - Building Automation System (BAS)
  - Building Lighting System (Lighting/Daylighting/Occupancy Control System)
  - Conveyance/Vertical Transport System (Elevators)
  - Electrical Systems (ES) [Such as local building generators not designed for grid interconnection, high reliability switching from two sources for critical buildings, etc.]
  - Heating, Ventilation, Air Conditioning (HVAC)
  - Irrigation System
  - SCADA
  - Shade Control System
  - Vehicle Charging System
- Fire & Life Safety - Owned and operated by Facilities
  - Fire Alarm Reporting System (FARS)
  - Fire Hydrant Water Distribution Systems
  - Fire Pump Control System
  - Mass Notification System (MNS)
- Traffic Control Systems
  - Traffic Signals Systems

# Assign Cyber Team

**CYBERSECURITY TEAM PERSONNEL**

The PROJECT Cybersecurity Team is comprised of highly skilled and certified IT and OT cybersecurity subject matter experts with extensive experience with the NIST Risk Management Framework and the DoD implementation of the RMF:

Cyber Team Lead: GICSP or CISSP
Cyber System Administrator: MCSE, Security +
Cyber Commissioning: CEM, CISSP, CEH, CxA, DGCP
Cyber Auditing: CDFM, CFE, CISA, CPA

The Cyber Team will be responsible for the project cyber lifecycle and will begin at project award with a Cyber Workshop Charette to baseline the PROJECT Team and **initiate the development of the RMF package documents, begin the auditing of the PROJECT Team's project NIST 800-171 Cyber Risk Management Plans (CRMP), create the Test and Development Environment (TDE), perform system hardening (SCAP/STIGS) of the equipment and components, create and manage the Fully-Mission Capable Baseline (FMC), perform sysadmin duties on the TDE and Production OT systems, audit the FRCS, and perform cyber commissioning of the facility.**

# Assemble the Stakeholders

The FRCS owner should assemble representatives from the following communities to participate in development of the FRCS PE authorization boundary and network architecture:

- Facility Engineer/Manager
- Facility Operations & Maintenance/Technician
- Physical Security Specialist
- Emergency Manager
- IT Network/Communications Specialist
- Information Assurance Specialist
- Tenants (Defense Health Agency, Defense Logistics Agency, etc)
- Operations and Maintenance Contractors
- Control System Vendor/Integrators
- Information Assurance IA/RMF Contractor

# Cybersecurity Guideline Sequence

| Activity / Lead | New Project | Renovation Project | Typical Duration |
|---|---|---|---|
| **Presolicitation RFP Considerations** | Obtain the Regional and ESTCP Platform Enclaves catogorization and categorize the CS | Obtain the Regional and ESTCP Platform Enclaves catogorization and categorize the CS | NA |
| **Design**<br>• Basis of Design<br>• Concept Design (10-15%)<br>• Design Development (35-50%)<br>• Pre-Final (90%)<br>• Final (100%)<br>Lead: A/E<br>Documents/Models/Tools:<br>• Construction Design Documents / Building Information Model (BIM) / CAD<br>• CSET<br>• GrassMarlin<br>• Draft Baseline System Security Plan (SSP)<br>• IT Contingency Plan and CONOPS (ITCP) | CS front end or new susbsystem back end to connect to front end<br>Confirm/revise system categorization, define network architecture, system components, concept of operations, drawings, and specifications.<br>At 90% design create initial SSP and baseline security risk assessment. | CS front end upgrade or subsystem modernization<br>Confirm/revise system categorization, define network architecture, system components, concept of operations, drawings, and specifications.<br>At 90% design create initial SSP and baseline secuirty risk assessment. | 3-6 Months |

# Cybersecurity Guideline TDE

**TEST AND DEVELOPMENT ENVIRONMENT** For new or major modernization projects, the **Systems Integrator will establish a Test and Development Environment (TDE) that replicates the Production Environment to the highest degree possible starting with the Level 4 Workstations, Servers, software and with at least one of each of the Level 3-0 major components, devices, and actuators.** At approximately the 50-75% construction complete, the TDE will be used to perform Factory Acceptance Testing (FAT) of the project to ensure the project has end-to-end functionality, has been properly configured using the Security Content Automation Protocol (SCAP) tool and the Security Technical Implementation Guides (STIGS), all patches (OS and FRCS) are installed and properly configured, and begin creating the artifacts for the draft System Security Plan.

At approximately 95-100% construction complete, the TDE will be used to conduct Site Acceptance Testing of the complete FRCS, and if required, Penetration testing. The SAT artifacts will be included in the final System Security Plan, FMC and Jump-Kit (if required).

The ESTCP Project Team/System Integrator will transfer the TDE to the ESTCP PM for inclusion into the Platform Enclave Operations Center.

# Facility Control Systems Ops Center

**Facility Control Systems Operations Center (FCSOC)**

**Coordinate with all responsible organizations to determine the location of the FRCS servers, central monitoring and operational control/Human Machine Interface (HMI) operator's consoles, and the Test and Development Environment (TDE).** The FCSOC can be within the campus or located on the installation at other Operations Centers (SOC, Fire Department, NETCOM Network Operations Security Center, etc.). Identify if the PE servers, workstations, laptops, switches, routers, etc. (all "traditional IT Front-End") will be GFE or if contactor procured and installed and turned over to government. **All PE assets capable of being hardened using the Security Technical Implementation Guides (STIGS), will be configured and checked using the Factory Acceptance Testing/Site Acceptance Testing (FAT/SAT) Checklist.** Determine if penetration testing, and what type, will be required; the ESS is recommended to have penetration testing (High Impact) per NIST SP 800-82. Complete the EI&E Penetration Testing Checklist.

# RMF Cybersecurity SME Required

D3100 CYBERSECURITY
D310001 CYBERSECURITY SPECIALIST
Provide a dedicated Cybersecurity Specialist on the D/B team. The Cybersecurity Specialist is to be an individual or firm who is regularly and professionally engaged in the business of the applications, installation, and testing of the specified Cybersecurity and equipment required for this project. The Cybersecurity Specialist is to demonstrate experience in providing successful control system security protection within the past three years of similar scope and size**. The Cybersecurity Specialist is to design a system in accordance with contract requirements and ensure the design is fully implemented during construction**. Additionally the Cybersecurity Specialist is **responsible for creating the artifacts and documentation required to achieve RMF authorization.** Submit documentation for a minimum of three and a maximum of five successful control system installations for the Cybersecurity Specialist.

# USACE UMCS V APPENDIX B

1.0 Cybersecurity Requirements: **The contractor shall follow Unified Facility Criteria (UFC) 4-010-06 and Unified Facility Guide Specification (UFGS) 25 05 11, Cybersecurity of Facility-Related Control Systems.** UFC 4-010-06 defines the five steps to integrate cybersecurity into the FRCS Design as follows (see UFC 4-010-06 Chapter 3-1.1 Five Steps for Cybersecurity Design):

1.1 **The Contractor shall provide a cyber-secure system(s) with all applicable security artifacts and security engineering to meet the requirements of receiving an ATO accreditation decision via the DoD RMF.** The implementation of cybersecurity measures in relation to design and construction / installation of the system shall not impede the system's functional requirements. However, cybersecurity measures should be applied to the greatest extent possible and where compliance cannot be met, deviations from cybersecurity standards should be documented and appropriately justified. The expected duration for RMF Activities 1-5 stated below shall be approximately 12 months. The Contractor shall conduct and participate in RMF meetings as required by the PWS.

# New Contract Language from Air Force

Upon completion of RMF Step 2, (at the 60% Design Phase Submittal, and all subsequent Design Phase Submittals) the **A-E shall provide the following as deliverables:**

a) Updated Draft Security Plan with security controls and CCIs determined in this step, along with other artifacts provided by the System Owner

b) Edited guide specifications to include UFGS 25 05 11 and other specification sections with affected control systems

c) **Cybersecurity section in the Design Analysis which includes**:

Overview and description of cybersecurity requirements for this project . Draft Security Plan . Interview with site personnel/occupants and resulting recommendations . Review of Master Plan (if any) . Field survey data . Survey of existing data communication infrastructure . Proposed data communication system (include routers/switches) . Existing front-end system protocol and interface requirements . Integration to existing system technical solution (if any) . Network Architecture including the proposed network IP ports, protocols, and services associated with the facility related control system . Workstation/server . Preliminary system components

# Cyber Commissioning

- Unified Facilities Guide Specifications (UFGS) 25 05 11 Cybersecurity Of Facility-Related Control Systems Contractor Computer Cybersecurity Compliance Statement - For each contractor-owned computer, list the make and model of the device, the device serial number, the operating system version, and the anti-malware software version. Attach additional sheets if required to document all computers.
- Unified Facilities Guide Specifications (UFGS) 25 05 11 Cybersecurity Of Facility-Related Control Systems Cybersecurity Schedules – consists of four tabs to be completed; Interconnection Schedule, Network Communication Schedule, Wireless, and Multiple IP Connection.
- Unified Facilities Guide Specifications (UFGS) 25 05 11 Cybersecurity Of Facility-Related Control Systems Inventory Spreadsheet - Provide a Control System Inventory report using the Inventory Spreadsheet listed under this Section documenting all [networked devices, including network infrastructure devices] [devices, including networked devices, network infrastructure devices, non-networked devices, input devices (e.g. sensors) and output devices (e.g. actuators)]. For each device provide all applicable information for which there is a field on the spreadsheet in accordance with the instructions on the spreadsheet.
- Unified Facilities Guide Specifications (UFGS) 25 05 11 Cybersecurity Of Facility-Related Control Systems Contractor Temporary Network Cybersecurity Compliance Statement - Provide a single submittal containing completed Contractor Computer Cybersecurity Compliance Statements for each company using contractor owned computers. Each Statement must be signed by a cybersecurity representative for the relevant company.

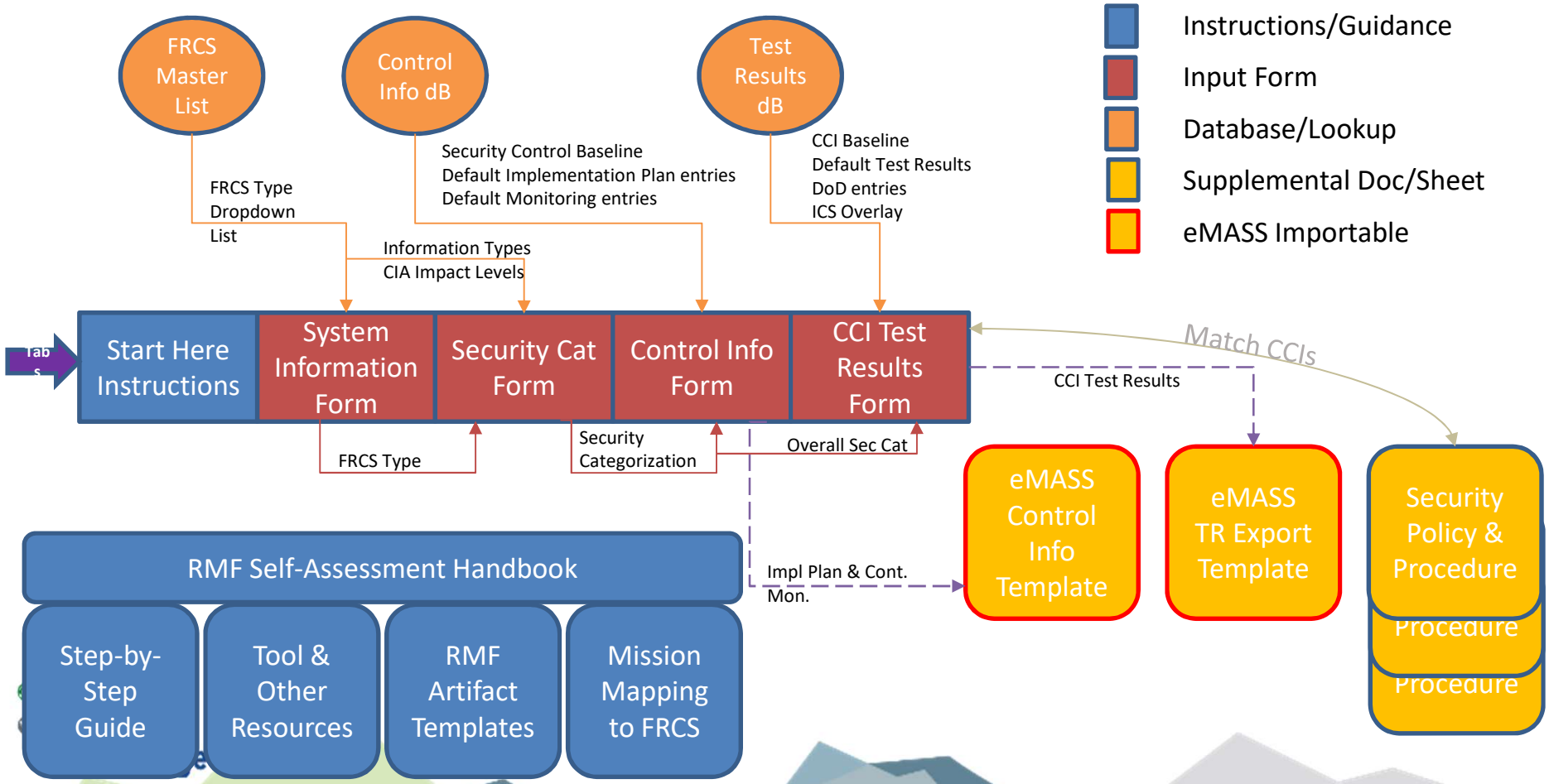
ure the OS and vendor
) are properly hardened using
s) and configured to the JIE
ce and turnover of the project
e.

is a functional recovery point
should capture the FMC
s, remote access terminals,
a flow, and machine/device
formation should be kept
anges are made to the
C baseline is used to
conditions of the FRCS. The
he initial FMC baseline.

ISCP and the FMC are used to perform disaster recovery and includes where back-ups are stored and the process to restore the FMC, the sequence of re-restart, assignment of personnel to the Roles and Responsibilities Table, and how to perform Functional and Validation Testing.

- System Security Plan (SSP) – Use the DoD Core Authorization Package to develop a Preliminary SSP.

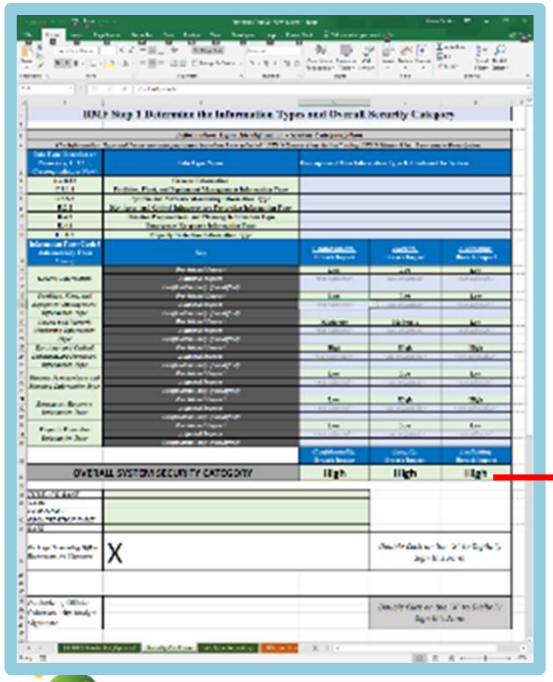
# ESCTP FRCS RMF Tool – Coming Soon!



# ESCTP FRCS RMF Tool

Step 3
Implement Controls

## CCI Test Results Form

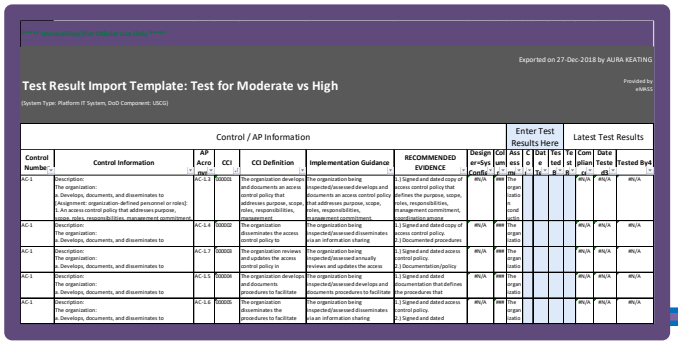


Security Categorization Form

NIST 800-82
800-82 ICS
Overlay

DoD-level Policies

UFC 4-010-06




eMASS Import of Test Results

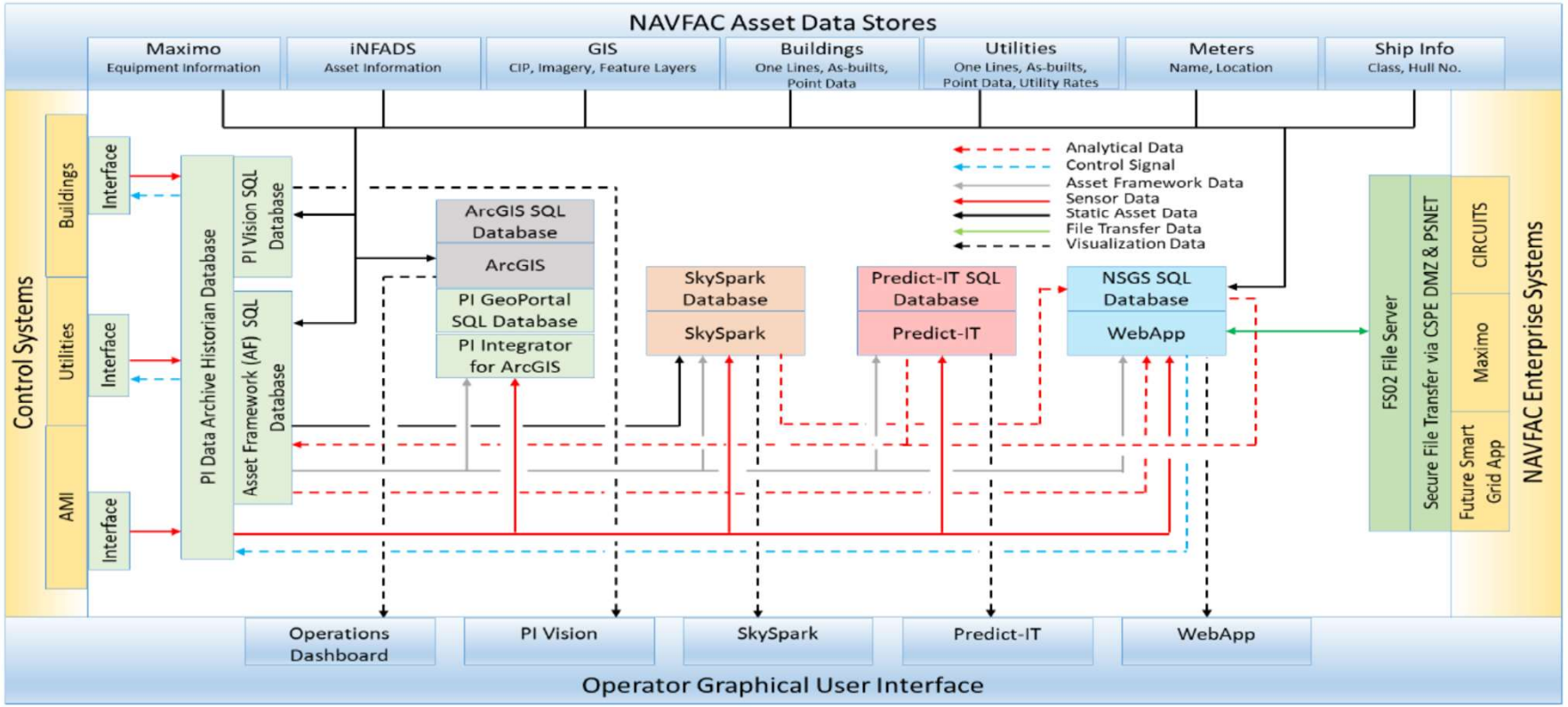
**Test Result Export Form**

- eMASS format
- Autofill of CCI Test Results to apply ICS Overlay
- Autofill of CCI Test Results for DoD-level policies
- Autofill of CCI Test Results with UFC 4-010-06 supplemental controls to ICS Overlay
- Auto-color to identify remaining User input fields
- Excel formula provided to pull tool data into eMASS template for import

27

# Navy Smart Grid

## Smart Grid System Description





Tara Houlden

NAVFAC Cybersecurity Director

Kevin Whitt

KBR Smart Grid Project Manager


Energy Exchange 2019

# Navy Smart Grid Lessons Learned

Standardized Enterprise Architecture, the NAVFAC Control System Platform Enclave (CSPE), facilitated Smart Grid development.

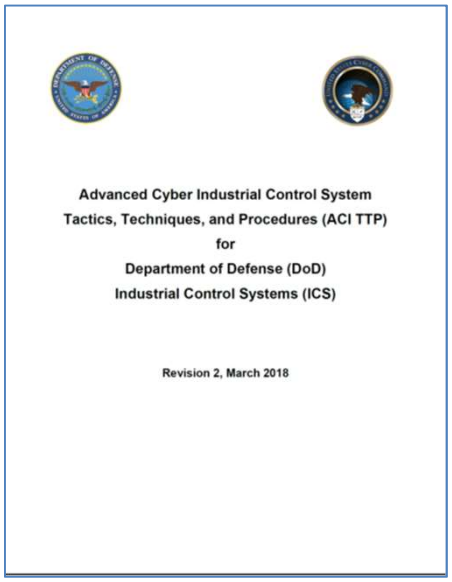
- Standard Regional Deployments
- Established communications with FRCS via Base Area Networks (BAN)
- Connection agreements with Public Safety Network (PSNet) established communication links with Navy Installation BANs within regions
- PSNet architecture enables secure communication between the CSPE and the NAVFAC business system environment
- Provided SG hosting environment with numerous inherited controls
- Created economical platform for SG development and deployment

Tara Houlden
NAVFAC Cybersecurity Director
Kevin Whitt
KBR Smart Grid Project Manager

Energy Exchange 2019

# ACI TTP for DoD ICS V2 Mar 2018

The scope of the ACI TTP includes all DoD ICS. DoD ICS, which include **supervisory control and data acquisition (SCADA) systems, distributed control systems (DFRCS),** and other control system configurations, such as skid-mounted programmable logic controllers (PLC) are typical configurations found throughout the DoD. **ICS are often used in the DoD to manage sectors of critical infrastructure such as electricity, water, wastewater, oil and natural gas, and transportation.**


Advanced Cyber Industrial Control System
Tactics, Techniques, and Procedures (ACI TTP)
for
Department of Defense (DoD)
Industrial Control Systems (ICS)

Revision 2, March 2018

**3. How to Use These TTP**

This ACI TTP is divided into essentially four sections:

- **ACI TTP Concepts** (chapters 2 through 4)
- **Threat-Response Procedures** (**Detection, Mitigation, Recovery**) (enclosures A, B, and C)
- **Routine Monitoring of the Network and Baselining the Network** (enclosures D and E)
- **Reference Materials** (enclosures F through I and appendix A through D)

**DSD Memo Jul 2018 (FOUO)**

SUBJECT: Enhancing Cybersecurity Risk Management for Control Systems Supporting DoD-Owned Defense Critical Infrastructure

**Begin using the ACI TTP…..**

# Switching Gears….

**252.204-7008 COMPLIANCE WITH SAFEGUARDING COVERED DEFENSE INFORMATION CONTROLS (OCT 2016)**

# DFARS 254.204-7012

252.204-7008 COMPLIANCE WITH SAFEGUARDING COVERED DEFENSE INFORMATION CONTROLS (OCT 2016)

(a) Definitions. As used in this provision--

Controlled technical information, covered contractor information system, covered defense information, cyber incident, information system, and technical information are defined in clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting.

(b) **The security requirements required by contract clause 252.204-7012 shall be implemented for all covered defense information on all covered contractor information systems that support the performance of this contract.**

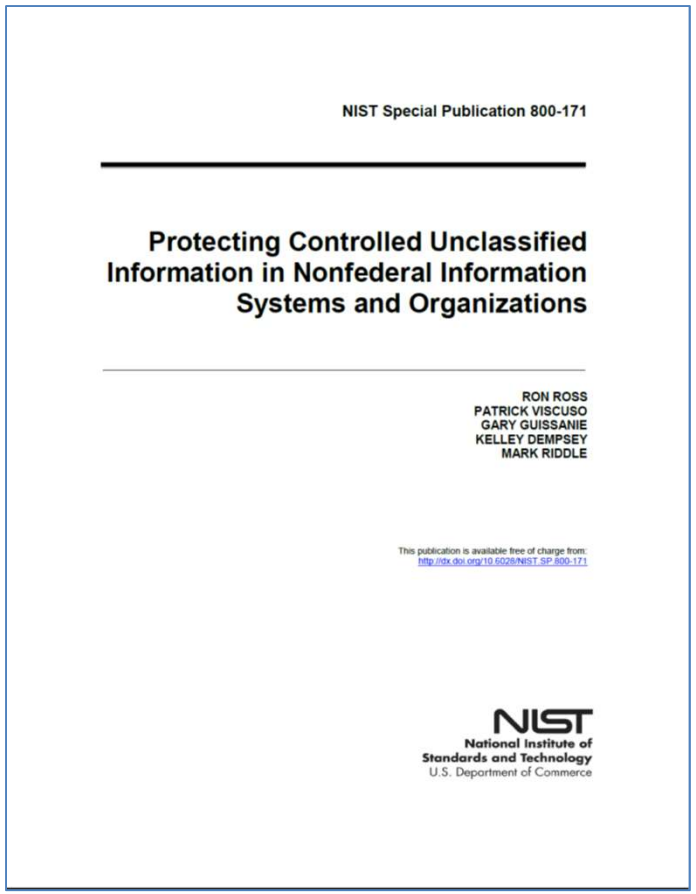
(c) For covered contractor information systems that are not part of an information technology service or system operated on behalf of the Government (see 252.204-7012(b)(2))--

(1) By submission of this offer**, the Offeror represents that it will implement the security requirements specified by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, ``Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations''** (see http://dx.doi.org/10.6028/NIST.SP.800-171) that are in effect at the time the solicitation is issued or as authorized by the contracting officer not later than December 31, 2017.

# ESTCP FRCS Protecting CUI

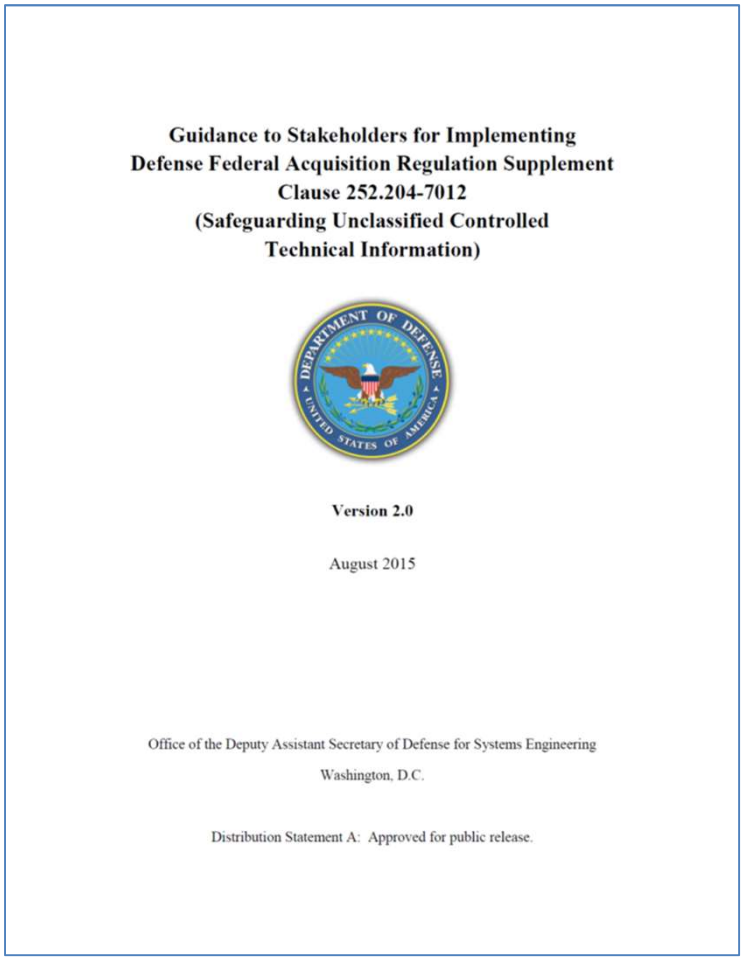

https://serdp-estcp.org/Tools-and-Training/Installation-Energy-and-Water/Cybersecurity/FRCS-Protecting-CUI

# NIST SP 800-171 CRMP




**The protection of Controlled Unclassified Information (CUI) while residing in nonfederal information systems and organizations is of paramount importance to federal agencies** and can directly impact the ability of the federal government to successfully carry out its designated missions and business operations. **The requirements apply to all components of nonfederal information systems and organizations that process, store, or transmit CUI, or provide security protection for such components.** The CUI requirements are intended for use by federal agencies in contractual vehicles or other agreements established between those agencies and nonfederal organizations.

# DFARS Safeguarding CUI 2015



Guidance to Stakeholders for Implementing
Defense Federal Acquisition Regulation Supplement
Clause 252.204-7012
(Safeguarding Unclassified Controlled
Technical Information)

Version 2.0

August 2015

Office of the Deputy Assistant Secretary of Defense for Systems Engineering

Washington, D.C.

Distribution Statement A: Approved for public release.

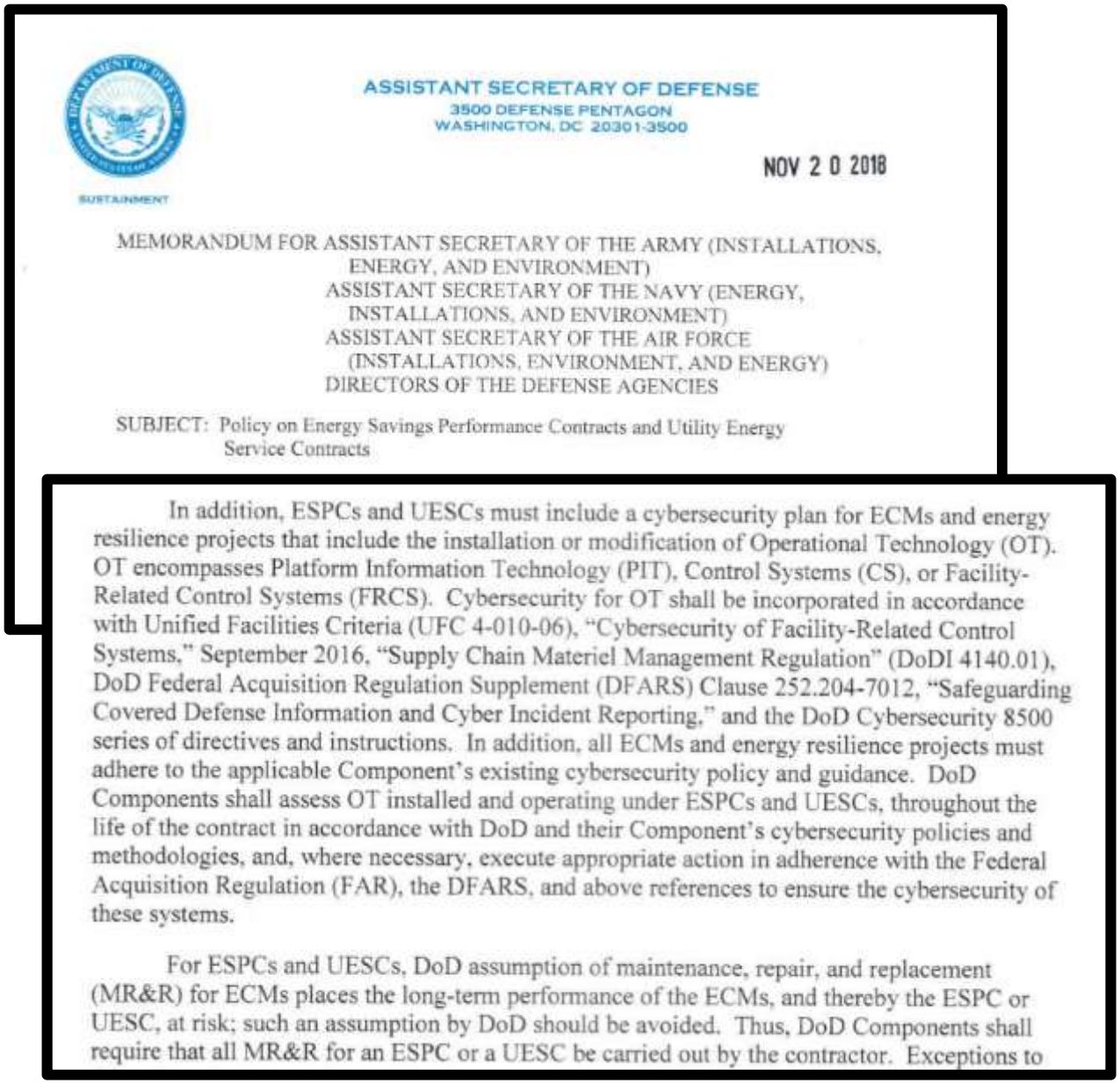
**1.0 Purpose**

This guidance is intended for stakeholders charged with **protection of unclassified controlled technical information (CTI) resident on or transiting through contractor information system(s)** covered by DFARS 252-204-7012 (Safeguarding Unclassified Controlled Technical Information). CTI is technical information with military or space application that is subject to controls on its access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. This guide will assist stakeholders in carrying out their responsibilities **should a defense contractor report a compromise on a contract that contains unclassified CTI.**

# DFARS Technical Information

- Technical data or computer software as defined in DFARS Clause 252.227-7013, Rights in Technical Data-Non Commercial Items, regardless of whether or not the clause is incorporated in the solicitation or contract. Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.
- **The data may be in tangible form, such as a blueprint, photograph, plan, instruction, or an operating manual, or may be intangible, such as a technical service or oral, auditory, or visual descriptions.**
- **Examples of technical data include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software.**

# ASD Memo For ESPC and UESC



ASSISTANT SECRETARY OF DEFENSE
3500 DEFENSE PENTAGON
WASHINGTON, DC 20301-3500

NOV 2 0 2018

SUSTAINMENT

MEMORANDUM FOR ASSISTANT SECRETARY OF THE ARMY (INSTALLATIONS, ENERGY, AND ENVIRONMENT)
ASSISTANT SECRETARY OF THE NAVY (ENERGY, INSTALLATIONS, AND ENVIRONMENT)
ASSISTANT SECRETARY OF THE AIR FORCE (INSTALLATIONS, ENVIRONMENT, AND ENERGY)
DIRECTORS OF THE DEFENSE AGENCIES

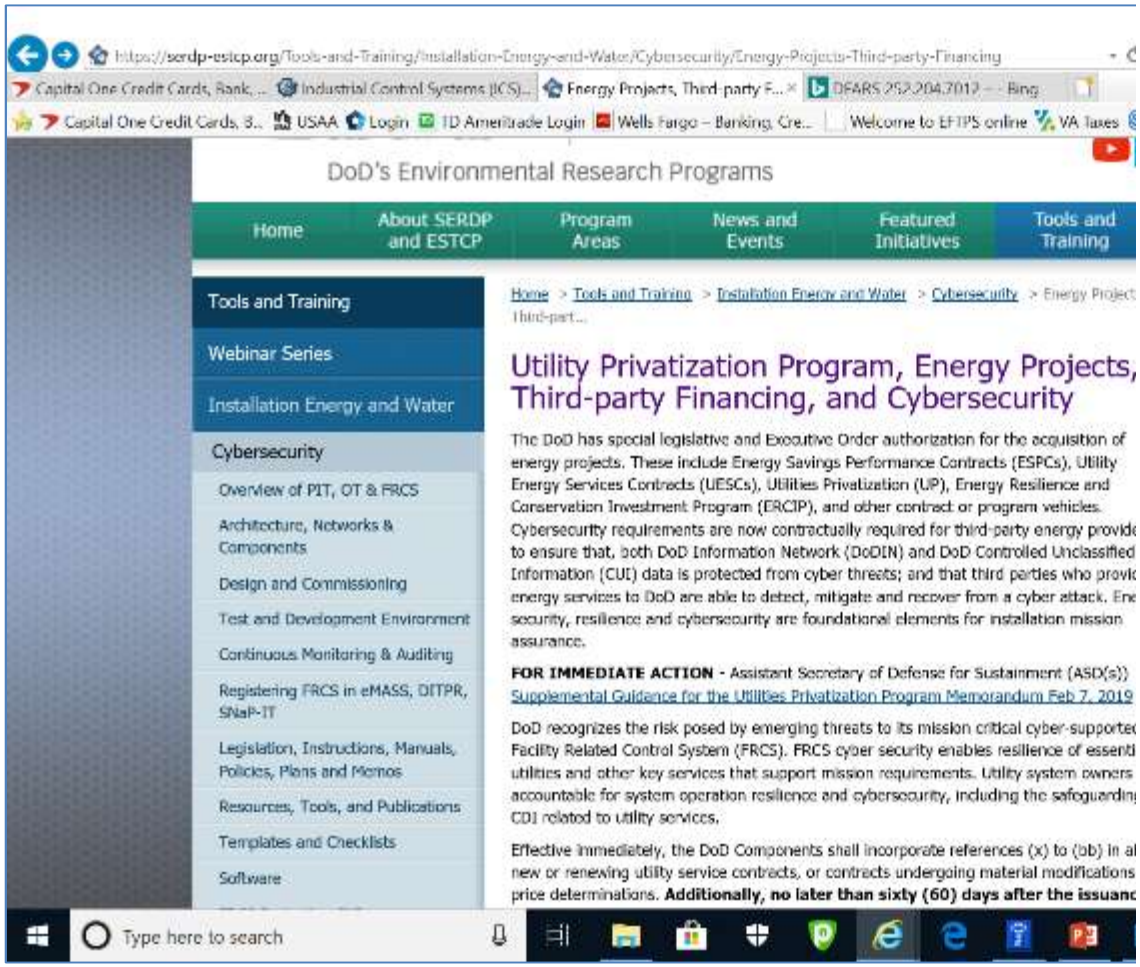
SUBJECT: Policy on Energy Savings Performance Contracts and Utility Energy Service Contracts

In addition, ESPCs and UESCs must include a cybersecurity plan for ECMs and energy resilience projects that include the installation or modification of Operational Technology (OT). OT encompasses Platform Information Technology (PIT), Control Systems (CS), or Facility-Related Control Systems (FRCS). Cybersecurity for OT shall be incorporated in accordance with Unified Facilities Criteria (UFC 4-010-06), "Cybersecurity of Facility-Related Control Systems," September 2016, "Supply Chain Materiel Management Regulation" (DoDI 4140.01), DoD Federal Acquisition Regulation Supplement (DFARS) Clause 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting," and the DoD Cybersecurity 8500 series of directives and instructions. In addition, all ECMs and energy resilience projects must adhere to the applicable Component's existing cybersecurity policy and guidance. DoD Components shall assess OT installed and operating under ESPCs and UESCs, throughout the life of the contract in accordance with DoD and their Component's cybersecurity policies and methodologies, and, where necessary, execute appropriate action in adherence with the Federal Acquisition Regulation (FAR), the DFARS, and above references to ensure the cybersecurity of these systems.

For ESPCs and UESCs, DoD assumption of maintenance, repair, and replacement (MR&R) for ECMs places the long-term performance of the ECMs, and thereby the ESPC or UESC, at risk; such an assumption by DoD should be avoided. Thus, DoD Components shall require that all MR&R for an ESPC or a UESC be carried out by the contractor. Exceptions to

**All data required to provide privatized utility services" be handled as Covered Defense Information/Controlled Unclassified Data – new, renewing, and existing utility service contracts**

# DoD ESCTP Cybersecurity FRCS




https://serdp-estcp.org/Tools-and-Training/Installation-Water/Cybersecurity/Energy-Projects-Third-party-Finan

**FOR IMMEDIATE ACTION** - Assistant Secretary of Defense for Sustainment (ASD(s)) Supplemental Guidance for the Utilities Privatization Program Memorandum Feb 7, 2019. DoD recognizes the risk posed by emerging threats to its mission critical cyber-supported Facility Related Control System (FRCS). FRCS cyber security enables resilience of essential utilities and other key services that support mission requirements. **Utility system owners are accountable for system operation resilience and cybersecurity, including the safeguarding of CDI related to utility services**

# Cybersecurity of Energy Control Systems

**Cybersecurity of Energy Control Systems and Data**

Each Third-Party energy project will have unique operational and cybersecurity requirements depending on the local market energy resources (nuclear, coal, solar, wind, thermal, etc.), the Independent System Operator (ISO), and the Regional Transmission Office (RTO) and the DoD Interconnect to the local grid as shown in Figure 2.

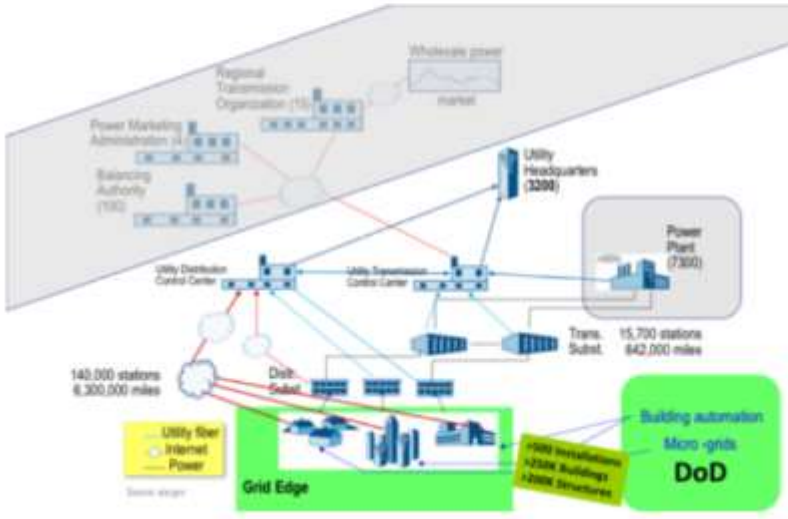


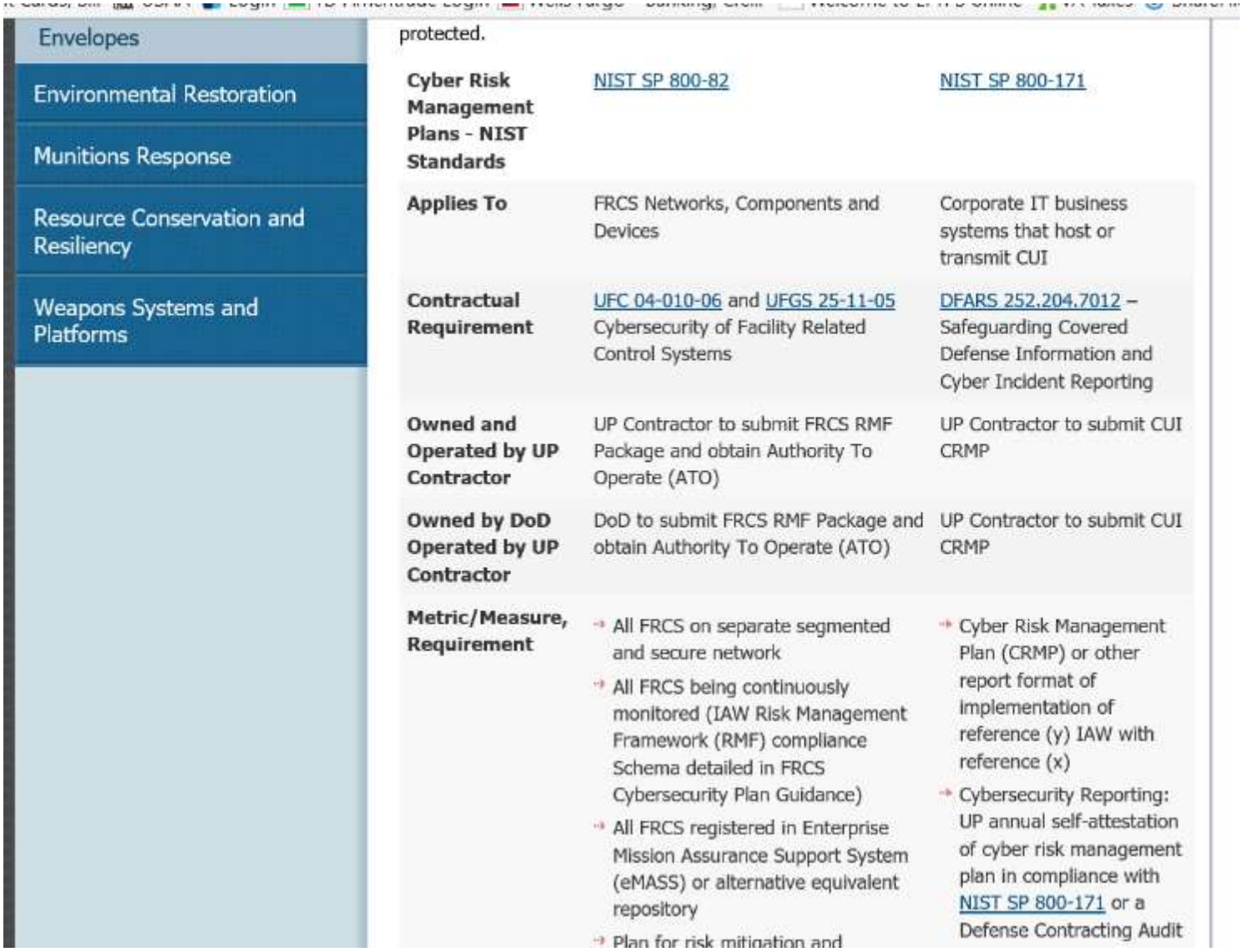

Figure 2 – DoD Energy Data Flows

From the Facility-Related Control Systems Master List; for Utility Control Systems, Building Control Systems, or Utility Monitoring and Control Systems, the following Data and Information Types are applicable to energy projects (the System Owner and Authorizing Official make final determination):

- C.2.8.12 General Information
- C.3.1.1 Facilities, Fleet, and Equipment Management Information Type
- C.3.5.8 System and Network Monitoring Information Type
- D.2.2 Key Asset and Critical Infrastructure Protection Information Type
- D.7.1 Energy Supply Information Type

https://serdp-estcp.org/Tools-and-Training/Installation-Energy-and-Water/Cybersecurity/Energy-Projects-Third-party-Financing

# Cyber Risk Plans for Business and CS



- Envelopes
- Environmental Restoration
- Munitions Response
- Resource Conservation and Resiliency
- Weapons Systems and Platforms

protected.

| | | |
|---|---|---|
| **Cyber Risk Management Plans - NIST Standards** | NIST SP 800-82 | NIST SP 800-171 |
| **Applies To** | FRCS Networks, Components and Devices | Corporate IT business systems that host or transmit CUI |
| **Contractual Requirement** | UFC 04-010-06 and UFGS 25-11-05 Cybersecurity of Facility Related Control Systems | DFARS 252.204.7012 – Safeguarding Covered Defense Information and Cyber Incident Reporting |
| **Owned and Operated by UP Contractor** | UP Contractor to submit FRCS RMF Package and obtain Authority To Operate (ATO) | UP Contractor to submit CUI CRMP |
| **Owned by DoD Operated by UP Contractor** | DoD to submit FRCS RMF Package and obtain Authority To Operate (ATO) | UP Contractor to submit CUI CRMP |
| **Metric/Measure, Requirement** | → All FRCS on separate segmented and secure network<br>→ All FRCS being continuously monitored (IAW Risk Management Framework (RMF) compliance Schema detailed in FRCS Cybersecurity Plan Guidance)<br>→ All FRCS registered in Enterprise Mission Assurance Support System (eMASS) or alternative equivalent repository<br>→ Plan for risk mitigation and | → Cyber Risk Management Plan (CRMP) or other report format of implementation of reference (y) IAW with reference (x)<br>→ Cybersecurity Reporting: UP annual self-attestation of cyber risk management plan in compliance with NIST SP 800-171 or a Defense Contracting Audit |

https://serdp-estcp.org/Tools-and-Training/Installation-Energy-and-Water/Cybersecurity/Energy-Projects-Third-party-Financing

# DIBNet Incident Reporting Portal


https://dibnet.dod.mil/portal/intranet/

# DIBNet Incident Reporting Portal

**3.1.1 DFARS Cyber Incident Reports**

DFARS cyber incidents are reported to the Defense Cyber Crime Center (DC3) via the DIBNet portal4. *Note: DIBNet is a web portal for sharing threat information between DoD and DIB companies.* See appendix F for a list of reportable fields.

**If the contractor does not have all the information required by the clause within the 72-hour time constraint**, specified in paragraph (d)(1) of the safeguarding clause, the contractor should report the details available at the time.

# Cybersecurity Maturity Model Certification

The Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)) recognizes that security is foundational to acquisition and should not be traded along with cost, schedule, and performance moving forward. The Department is committed to working with the Defense Industrial Base (DIB) sector to enhance the protection of controlled unclassified information (CUI) within the supply chain.

OUSD(A&S) is working with DoD stakeholders, University Affiliated Research Centers (UARCs), Federally Funded Research and Development Centers (FFRDC), and industry to develop the Cybersecurity Maturity Model Certification (CMMC).

**The CMMC will review and combine various cybersecurity standards and best practices and map these controls and processes across several maturity levels that range from basic cyber hygiene to advanced.** For a given CMMC level, the associated controls and processes, when implemented, will reduce risk against a specific set of cyber threats.

- The CMMC effort builds upon existing regulation (DFARS 252.204-7012) that is based on trust by adding a verification component with respect to cybersecurity requirements.
- **The goal is for CMMC to be cost-effective and affordable for small businesses to implement at the lower CMMC levels.**
- **The intent is for certified independent 3rd party organizations to conduct audits and inform risk.**

https://www.acq.osd.mil/cmmc/index.html

# Cybersecurity Maturity Model Certification

| | Description of Practices | Description of Processes |
|---|---|---|
| **Level 1** | • Basic cybersecurity<br>• Achievable for small companies<br>• Subset of universally accepted common practices<br>• Limited resistance against data exfiltration<br>• Limited resilience against malicious actions | • Practices are performed, at least in an ad-hoc matter |
| **Level 2** | • Inclusive of universally accepted cyber security best practices<br>• Resilient against unskilled threat actors<br>• Minor resistance against data exfiltration<br>• Minor resilience against malicious actions | • Practices are documented |
| **Level 3** | • Coverage of all NIST SP 800-171 rev 1 controls<br>• Additional practices beyond the scope of CUI protection<br>• Resilient against moderately skilled threat actors<br>• Moderate resistance against data exfiltration<br>• Moderate resilience against malicious actions<br>• Comprehensive knowledge of cyber assets | • Processes are maintained and followed |
| **Level 4** | • Advanced and sophisticated cybersecurity practices<br>• Resilient against advanced threat actors<br>• Defensive responses approach machine speed<br>• Increased resistance against and detection of data exfiltration<br>• Complete and continuous knowledge of cyber assets | • Processes are periodically reviewed, properly resourced, and improved across the enterprise |
| **Level 5** | • Highly advanced cybersecurity practices<br>• Reserved for the most critical systems<br>• Resilient against the most-advanced threat actors<br>• Defensive responses performed at machine speed<br>• Machine performed analytics and defensive actions<br>• Resistant against, and detection of, data exfiltration<br>• Autonomous knowledge of cyber assets | • Continuous improvement across the enterprise |

**A Level 4 CRMP can be created for approx. $5000 and include 2 audits and a Table-Top Exercise**

# QUESTIONS



**Tim Tetreault, PMP CEM**
**ESTCP Energy and Water Program Manager**
**4800 Mark Center Drive, Suite 16F16**
**Alexandria, VA 22350-3605**
**Office: 571-372-6397**
**Email: timothy.j.tetreault.civ@mail.mil**

**Daryl Haegley GICSP, OCP**
**Director, Mission Assurance & Deterrence**
**Principal Cyber Advisor to SECDEF**
**Mark Center 12G13 & Pentagon, 5D435**
**Office: 703-697-5766**
**Email: daryl.r.haegley.civ@mail.mil**

**Michael Chipley**
**President, The PMC Group LLC**
**Cell: 571-232-3890**
**E-mail: mchipley@pmcgroup.biz**