



- **Please note that microphones will be muted for the presentations**
- **Microphones will be opened for the 5 min Q&A for each presentation**

Emergency Preparedness and Infrastructure Resilience Committee Webinar for National Critical Infrastructure and Resilience Month

Featuring:

**Michael Chipley, PhD, PMP, LEED AP
The PMC Group LLC**

**Meredith Pringle
Converge Strategies**



The PMC Group LLC
Engineering a better tomorrow today





Society Centennial – 2020 – Washington D.C.



Society of American Military Engineers

Northern Virginia Post

14 November 2019

Welcome!



Announcements



- **2019 Upcoming SAME Events**
 - **Nov 20-22**, SAME SBC Federal Small Business Conference, Dallas, TX
 - www.same.org/calendar
 - **Dec 3**, 2019 LEADERSHIP AND MENTORING GRADUATION DINNER. Keynote Speaker: Wendell L. "Buddy" Barnes, PE, F.SAME, 100th SAME National President. 6:30PM - 9:30PM, The Waterford.
 - **Dec 12**, Monthly Luncheon - Regional Energy Panel of Speakers:
 - Ms Peggy Fox, Media and Community Relation Manager, Dominion Power
 - Mr Hardeep S. Rana, PE, AVP / Chief Engineer Corporate Engineering, Washington Gas

Note date change for December monthly luncheon!



Other Post Business



Other Upcoming Events / Announcements – www.same.org or www.same.org/NOVA

SAME Leader Development Program (LDP) – nominations open until Dec 2

NOVA Post Awards Program – Nominations being accepted for:

- Small Business of the Year
- Large Business of the Year
- Member of the Year
- Young Member of the Year
- COL (ret) Doug Lehmann Post Service Award

*Please send nominations for individual awards to Nick Desport at:
Nick.Desport@Merrick.com*



SAME Centennial



- SAME's Centennial Celebration, May 27-29, 2020, in Washington, D.C
 - Joint Engineer Training Conference & Expo
 - Walter E. Washington Convention Center
 - 75+ Continuing Education & Events
 - Engaging General Sessions with Keynote Speakers
 - Exhibit Hall – Booths, Historical Enhancements
 - 5th Annual Joint Engineer Table-Top Exercise
 - Society Ball & Awards Gala
 - Golden Eagle Awards
 - Early Bird Registration through February 28, 2020
 - More info at <https://www.samejetc.org/index.cfm>



Critical Infrastructure Security and Resilience Month



Official website of the Department of Homeland Security

CONTACT SITE MAP

CISA
CYBER-INFRASTRUCTURE

CYBERSECURITY INFRASTRUCTURE SECURITY EMERGENCY COMMUNICATIONS NATIONAL RISK MANAGEMENT ABOUT CISA MEDIA

Infrastructure Security > Critical Infrastructure Security and Resilience Month

Infrastructure Security

- 2015 Sector Specific Plans
- Critical Infrastructure Exercises
- Critical Infrastructure Security and Resilience Month**
- Chemical Security
- Critical Infrastructure Sector Partnerships
- Critical Infrastructure Training
- Critical Infrastructure Vulnerability Assessments
- Dams Sector Resources
- IDR Program
- Information Sharing: A Vital Resource
- Insider Threat Mitigation
- International Critical Infrastructure

CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE MONTH

Our American way of life—and the infrastructure that underpins it—is constantly evolving and growing in complexity and connectivity. These systems support the millions of activities that people conduct each day to transact business, communicate with friends and family, maintain health and safety, and more. They also include the venues where people gather to learn, worship, shop or find entertainment—in other words, the heart of our communities. These are all among the nation’s critical infrastructure systems, and without them, we would not have achieved our high level of national and economic security. For this reason, we observe Critical Infrastructure Security and Resilience Month each November.

Infrastructure Security Month is a time to shine a light on the vital role that critical infrastructure systems and places play in keeping the nation and our communities safe, secure and prosperous. It is also a time to think about how each of us can contribute to the security and resilience of the nation’s most essential services and functions—things like instant access to energy; safe, clean drinking water; reliable transportation; agriculture that supplies plentiful food year around; and even chemicals that are the building blocks of everything from plastics to electronics to fuel.

Every one of us has a role, whether it is investing in resilience, making preparedness plans—and exercising those plans, or simply saying something when you see something that looks suspicious.

Join us this November and take action to ensure our critical infrastructure is safe, secure, and resilient.

- Download your **Infrastructure Security Month** toolkit to get started.

To download Infrastructure Security Month images for use on your website or communications, please click the links below. *NOTE - These graphics should not be used to imply affiliation with or endorsement by the government.*

- Signature block
- Web banner (vertical)



<https://www.cisa.gov/infrastructure-security-month>

Homeland Security

Critical Infrastructure Security And Resilience Month
November 2018

FOLLOW NPPD ON SOCIAL MEDIA @NPPD

November is Critical Infrastructure Security and Resilience Month, an opportunity to highlight the efforts between Federal, State, local, territorial, and tribal governments and private sector partners to protect and secure our Nation’s critical infrastructure and enhance infrastructure resilience.


What Critical Infrastructure Means to You

The Nation’s critical infrastructure provides essential services that underpin American society and sustain the American way of life. We know critical infrastructure as the power we use in our homes and businesses, the water we drink, the transportation systems that get us from place to place, the first responders and hospitals in our communities, the farms that grow and raise our food, the stores we shop in, and the Internet and communication systems we rely on to stay in touch with friends and family.

Protecting and promoting the continuity of our Nation’s critical infrastructure is essential to our security, public health and safety, and economic vitality. Through a series of initiatives, Critical Infrastructure Security and Resilience Month reinforces the importance of critical infrastructure to America’s homeland security and economic prosperity and reiterates the Department’s commitment to keep our critical infrastructure, and the communities that depend on them, safe and secure. This requires a nationwide effort, with public and private partners working together toward a common goal.

Critical Infrastructure Security and Resilience Month activities can focus on several key areas to enhance security and resilience:

- Highlighting interdependencies between cyber and physical infrastructure.
- Pointing small and medium-sized businesses to the free tools and resources available to them to increase their security and resilience through Hometown Security and the four steps of Connect, Plan, Train, and Report (www.dhs.gov/hometown-security).
- Promoting public-private partnerships.
- Fostering innovation and investments in infrastructure resilience.
- Securing our Nation’s election infrastructure.



Risks to Critical Infrastructure

Critical infrastructure is increasingly at risk from a variety of threats, both natural and man-made, that continue to evolve—including climate change, extreme weather, aging and failing infrastructure components, cyberattacks, pandemics, and acts of terrorism. In particular, physical and cyber infrastructure have grown inextricably linked, meaning both cyber and physical measures are required to guard against the full array of threats. Growing interdependencies among infrastructure sectors and lifeline functions also impact the management of infrastructure risk. Understanding and mitigating these risks is a key element of our national security, resilience, economic prosperity.



Today's Event



**Emergency Preparedness and Infrastructure Resilience
Committee Webinar for National Critical Infrastructure and
Resilience Month
Featuring:**

**Michael Chipley, PhD, PMP, LEED AP -The PMC Group LLC
“Cybersecurity of Facility-Related Control Systems (FRCS) and
the DoD CIO Risk Management Framework”**



**Meredith Pringle - Converge Strategies
“Military Energy Resilience Catalyst (MERC) and Regional
Identification of Gaps in Operational Resilience (RIGOR)”**



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

November 14, 2019



FRCS Cyber and DFARS 254.204-7012

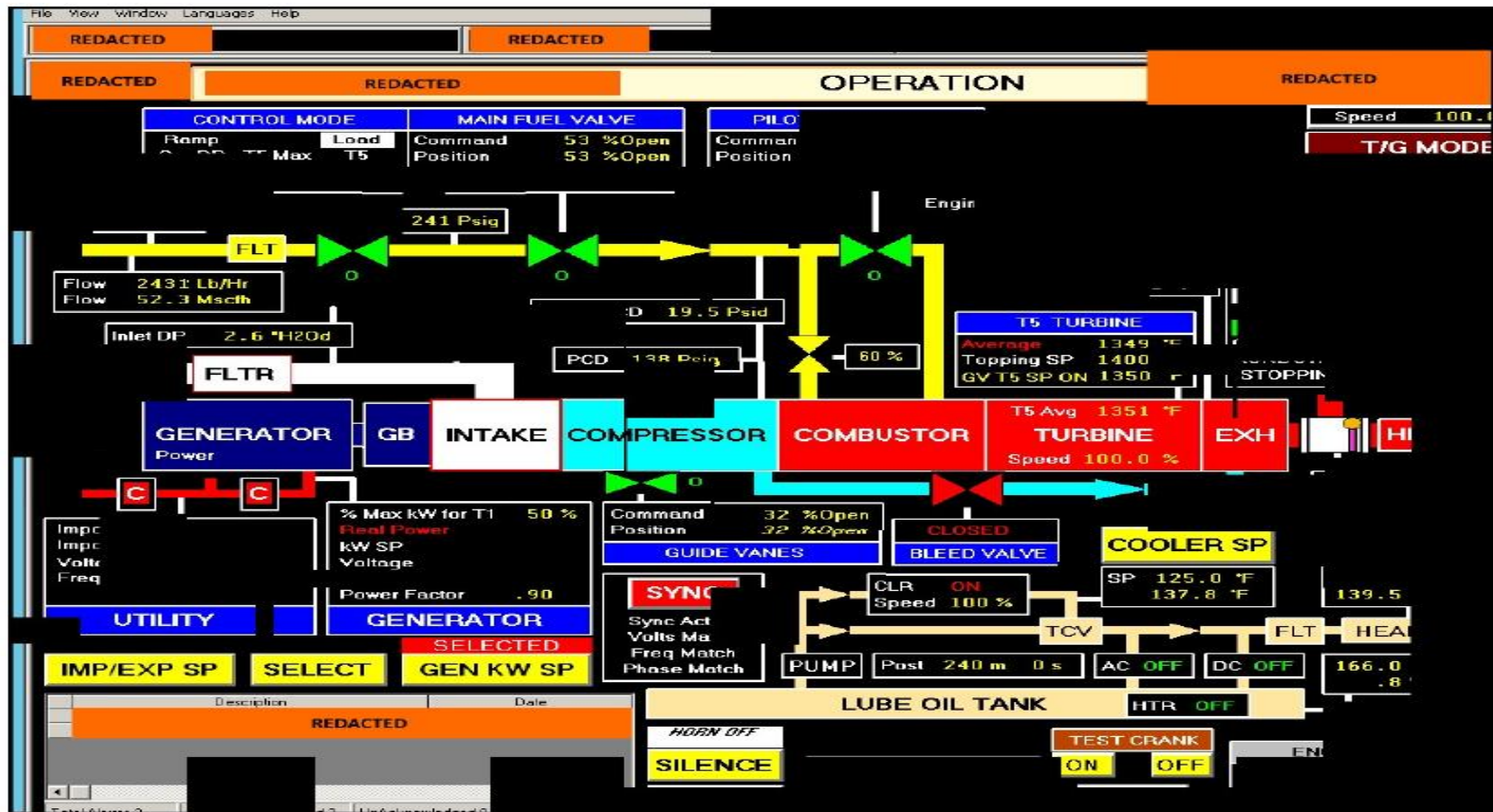
Today's Topics

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

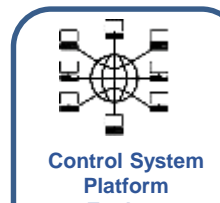
Russian Government Targeting Energy and Critical Infrastructure
March 2018 - Compromised control system screenshot below



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

DoD Facility Related Control Systems (FRCS)

Categories

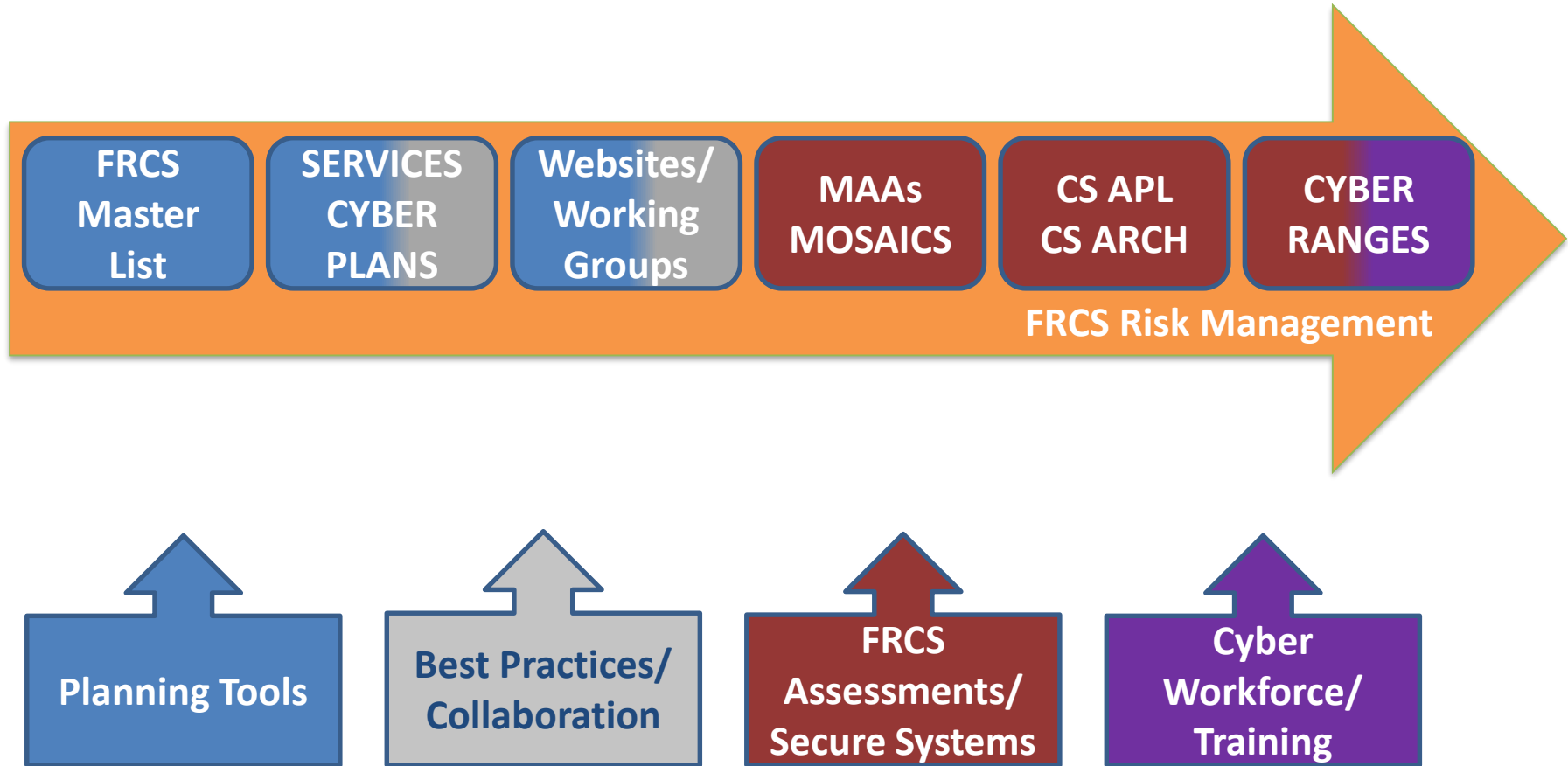


Systems

- 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?

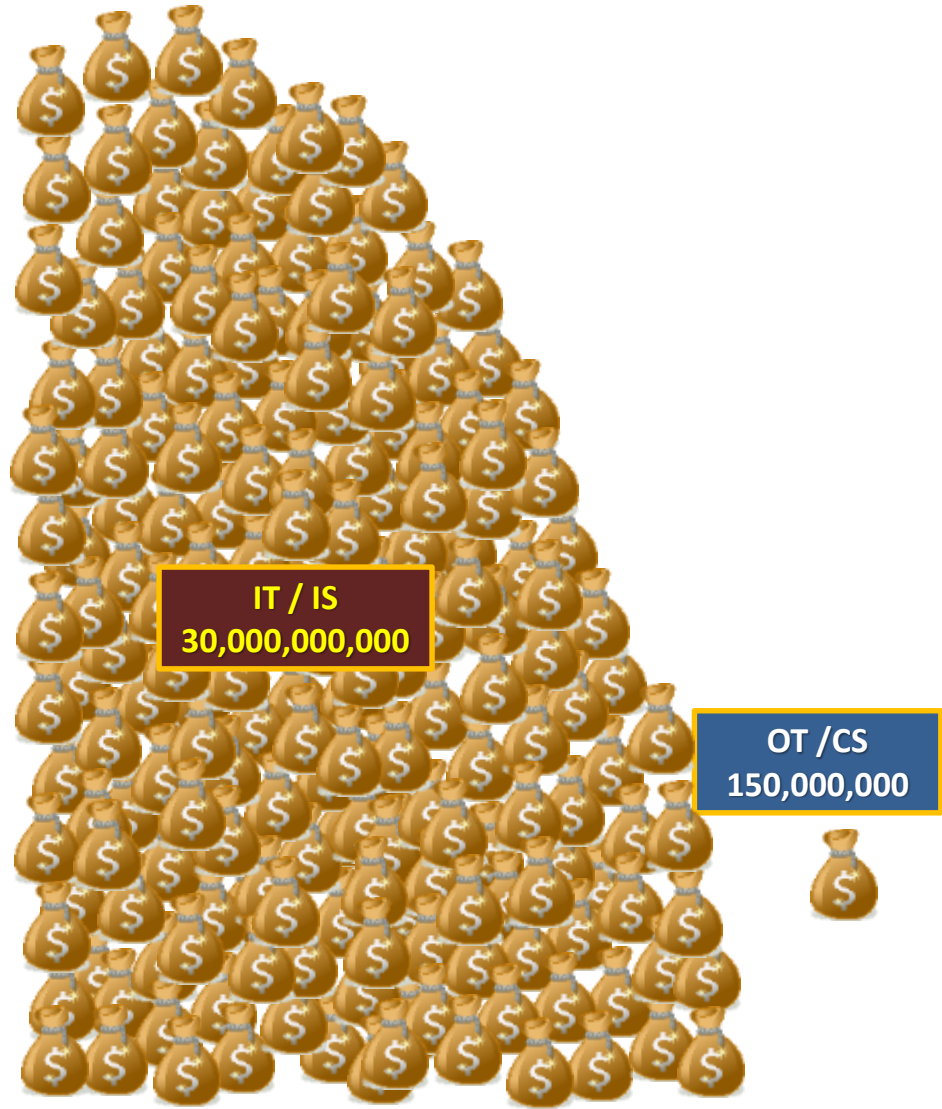
ODASD(E) Cybersecurity Initiatives



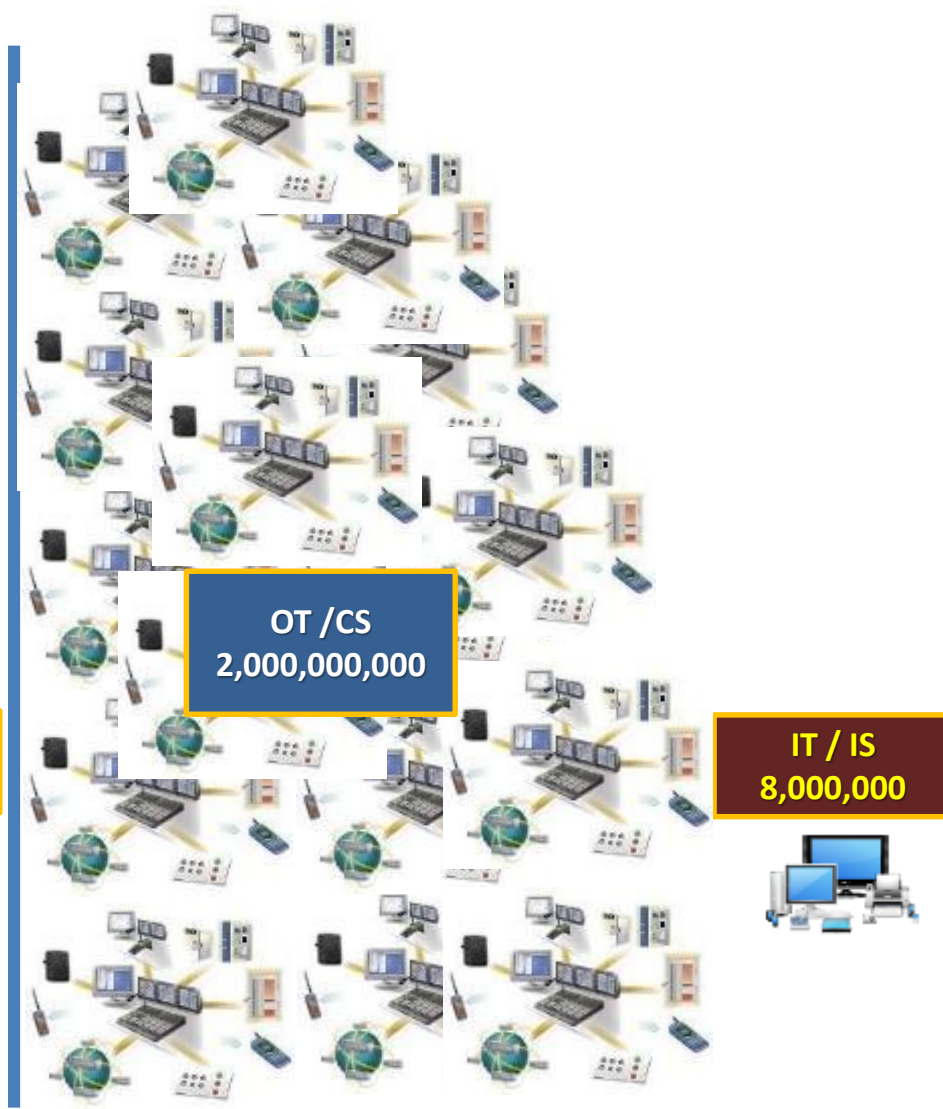
Alignment with Federal, Industry Objectives

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/Overview of PIT OT FRCS

Capital One Credit Cards, Bank... Industrial Control Systems (ICS)... Overview of PIT, OT & FRCS x DFARS 252.204.7012 -- Bing

Capital One Credit Cards, B... USAA Login TD Ameritrade Login Wells Fargo - Banking, Cre... Welcome to EFTPS online VA Taxes ShareFile - Where Compani... LinkedIn Cybersecurity WBDG Who...

SERDP DOD • EPA • DOE | **ESTCP**

DoD's Environmental Research Programs

SEARCH

Advanced search

View All Social Media

Home About SERDP and ESTCP Program Areas News and Events Featured Initiatives Tools and Training Funding Opportunities Investigator Resources

Tools and Training

Webinar Series

Installation Energy and Water

Cybersecurity

Overview of PIT, OT & FRCS

Architecture, Networks & Components

Design and Commissioning

Test and Development Environment

Continuous Monitoring & Auditing

Registering FRCS in eMASS, OITPR, SNAPEP

Legislation, Instructions, Manuals, Policies, Plans and Memos

Home > Tools and Training > Installation Energy and Water > Cybersecurity > Overview of PIT, OT & FRCS

Platform IT, Operational Technology and Facility-Related Control Systems

Department of Defense Instruction (DoDI) 8500.01, Cybersecurity, and DoDI 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT), incorporate Platform IT (PIT) into the RMF process. PIT is a category of both IT hardware and software that is physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems. PIT is further categorized as PIT products, PIT subsystems, or PIT systems. PIT differs from "traditional" IT in that it is integral to – and dedicated to the operation of – a specific platform. Although the term PIT is used only by DoD, the concept of categorizing components and systems dedicated to the operation of a specific platform is not. For example, within the private sector, the term "Operational Technology" (OT) is also used to refer to these systems and components.

The most common forms of Energy, Installation and Energy (Ei&E) PIT are Facility-Related Control Systems (FRCS), which are a combination of control components (e.g., electrical, mechanical, hydraulic, or pneumatic, etc.), special purpose controlling devices, and standard IT that act together upon underlying mechanical and/or electrical equipment to achieve an objective (e.g., transport of matter or energy, maintain a secure and comfortable work environment, etc.). All automated control systems are considered PIT. Industrial Control

PRINT

Program Areas

→ Installation Energy and Water

Featured Initiatives

→ Energy Assurance and Resilience

Share

Twitter

LinkedIn

Facebook

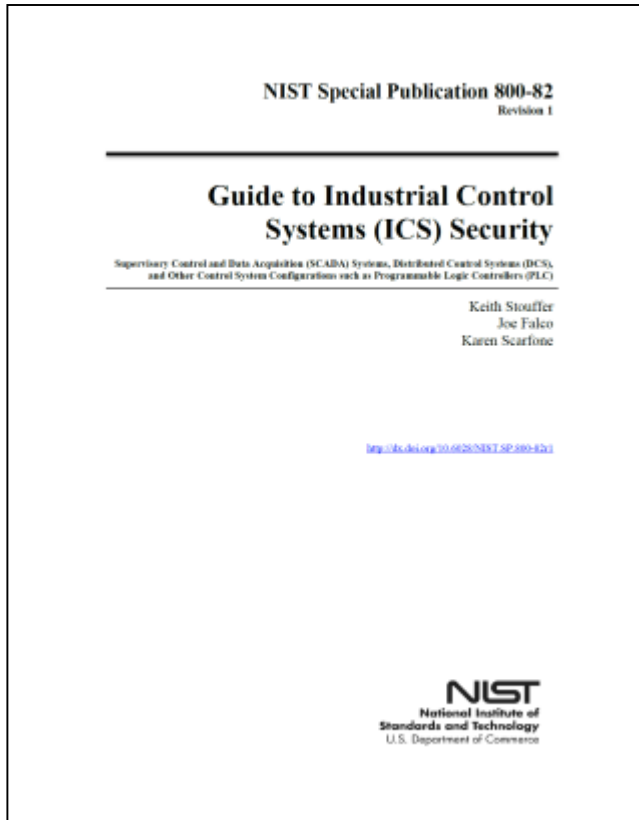
Email

Type here to search

3:34 PM 4/5/2019

<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

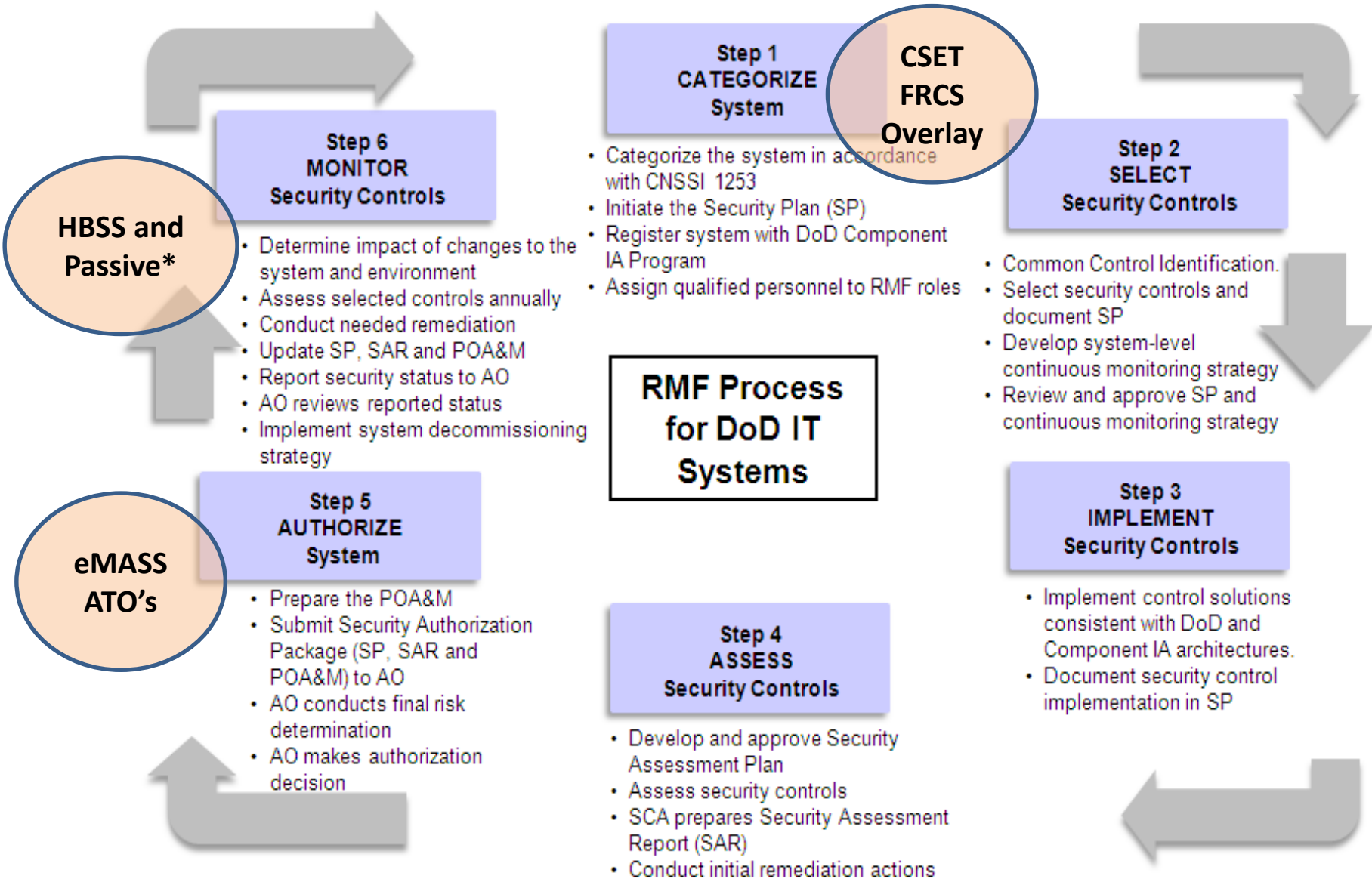
- CP-2 Contingency Plan
- CP-6 Alternate Storage Site
- CP-7 Alternate Processing Site
- CP-10 Information System Recovery and Reconstitution
- PE-3 Physical Access Control
- PE-10 Emergency Shutoff
- PE-11 Emergency Power
- PE-12 Emergency Lighting
- PE-13 Fire Protection
- PE-14 Temperature and Humidity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

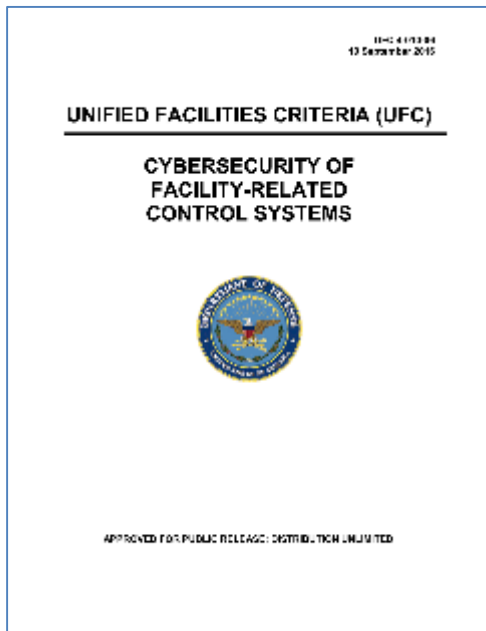
Inbound Protection,
Outbound Detection

FRCS Overlay & RMF Implementation



DoD UFC 4-010-06 Cybersecurity

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.

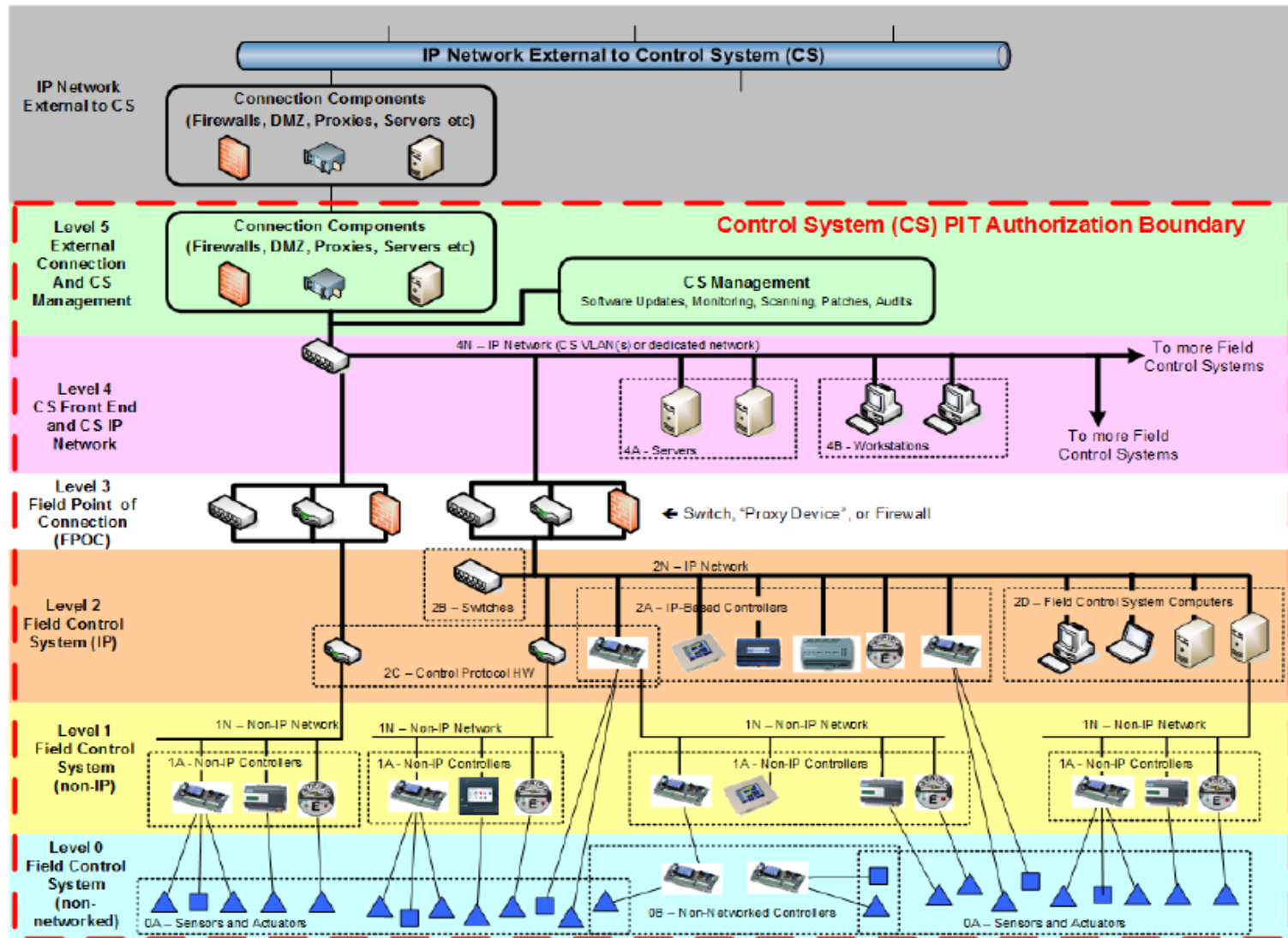
Step 3: Using the DoD master Control Correlation Identifier (CCI) list, **create a list of relevant CCIs** based on the controls selected in Step 2.

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

The screenshot shows a web browser window displaying the WBDG website. The address bar shows the URL: <http://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-25-05-11>. The browser tabs include 'UFGS 25 05 11 Cybersecurity...'. The website header features the WBDG logo, 'a program of the National Institute of Building Sciences', and navigation links: ABOUT, SITE MAP, CONTACT, CREATE ACCOUNT, LOGIN, and a search box labeled 'SEARCH WBDG'. A dark blue navigation bar contains links for DESIGN RECOMMENDATIONS, PROJECT MANAGEMENT - O & M, FEDERAL FACILITY CRITERIA (underlined), CONTINUING EDUCATION, and ADDITIONAL RESOURCES. The breadcrumb trail reads: DEPARTMENT OF DEFENSE / UNIFIED FACILITIES GUIDE SPECIFICATIONS (UFGS) / UFGS 25 05 11 CYBERSECURITY FOR FACILITY-RELATED CONTROL SYSTEMS. The main content area features the Department of Defense seal on the left and the title 'UFGS 25 05 11 CYBERSECURITY FOR FACILITY-RELATED CONTROL SYSTEMS' on the right. Below the title, the date is '11-01-2017', the division is 'Division 25 - Integrated Automation', and the page count is '50'. There are icons for PDF and ZIP download options. A 'RELATED LINKS' section is visible on the left. The Windows taskbar at the bottom shows the search bar, taskbar icons for File Explorer, Edge, Chrome, PowerPoint, Outlook, and Word, and system tray icons for network, volume, and date/time (7:45 AM 5/29/2018).

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

UFGS 25 05 11 Inventory

The screenshot displays the Microsoft Excel application window titled "UFGS 25 05 11 Inventory_Spreadsheet_2017-12-07 - Last Saved 5/3/2018 8:48 AM". The ribbon is set to "Home" and the active cell is M22. The spreadsheet is organized into four main sections:

- Device Location (Columns A-I):** Includes Identifier, Installation, Special Area, Facility Number or Identifier, Facility Name or Description, Floor, Room, Location in Room, and Enclosure or Mount Type.
- Control System Info (Columns J-N):** Includes UPS Power, Architecture Level, Control System Type, Part of which UMCS, and Electrical/Mechanical System or Equipment Controlled.
- HARDWARE DETAILS (Columns O-U):** Includes Device Type, Device Sub-Type, Device Function, Manufact. user, Product Line, Model #, and Serial #.
- OPERATING SYSTEM & PLATFORM (Columns V-Z):** Includes Type of Operating System (OS), OS Vendor, OS Name, OS Version, Platform Vendor, Platform Product Line, and Platform.

The spreadsheet is currently empty, with a small green selection box visible in cell M22. The Windows taskbar at the bottom shows the time as 2:15 PM on 12/14/2018.

UFGS 25 05 11 Schedules

The screenshot displays the Microsoft Excel interface with the following content in the spreadsheet:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
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 Communication 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																			
21																			

The spreadsheet tabs at the bottom are: Instructions, Interconnect, Network Comm, Wireless, Multiple_IP.

Create the Cyber Narrative

Cybersecurity

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

1

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 <ul style="list-style-type: none"> • Basis of Design • Concept Design (10-15%) • Design Development (35-50%) • Pre-Final (90%) • Final (100%) Lead: A/E Documents/Models/Tools: <ul style="list-style-type: none"> • Construction Design Documents / Building Information Model (BIM) / CAD • CSET • GrassMarlin • Draft Baseline System Security Plan (SSP) • IT Contingency Plan and CONOPS (ITCP) 	CS front end or new subsystem back end to connect to front end Confirm/revise system categorization, define network architecture, system components, concept of operations, drawings, and specifications. At 90% design create initial SSP and baseline security risk assessment.	CS front end upgrade or subsystem modernization Confirm/revise system categorization, define network architecture, system components, concept of operations, drawings, and specifications. At 90% design create initial SSP and baseline security 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:**

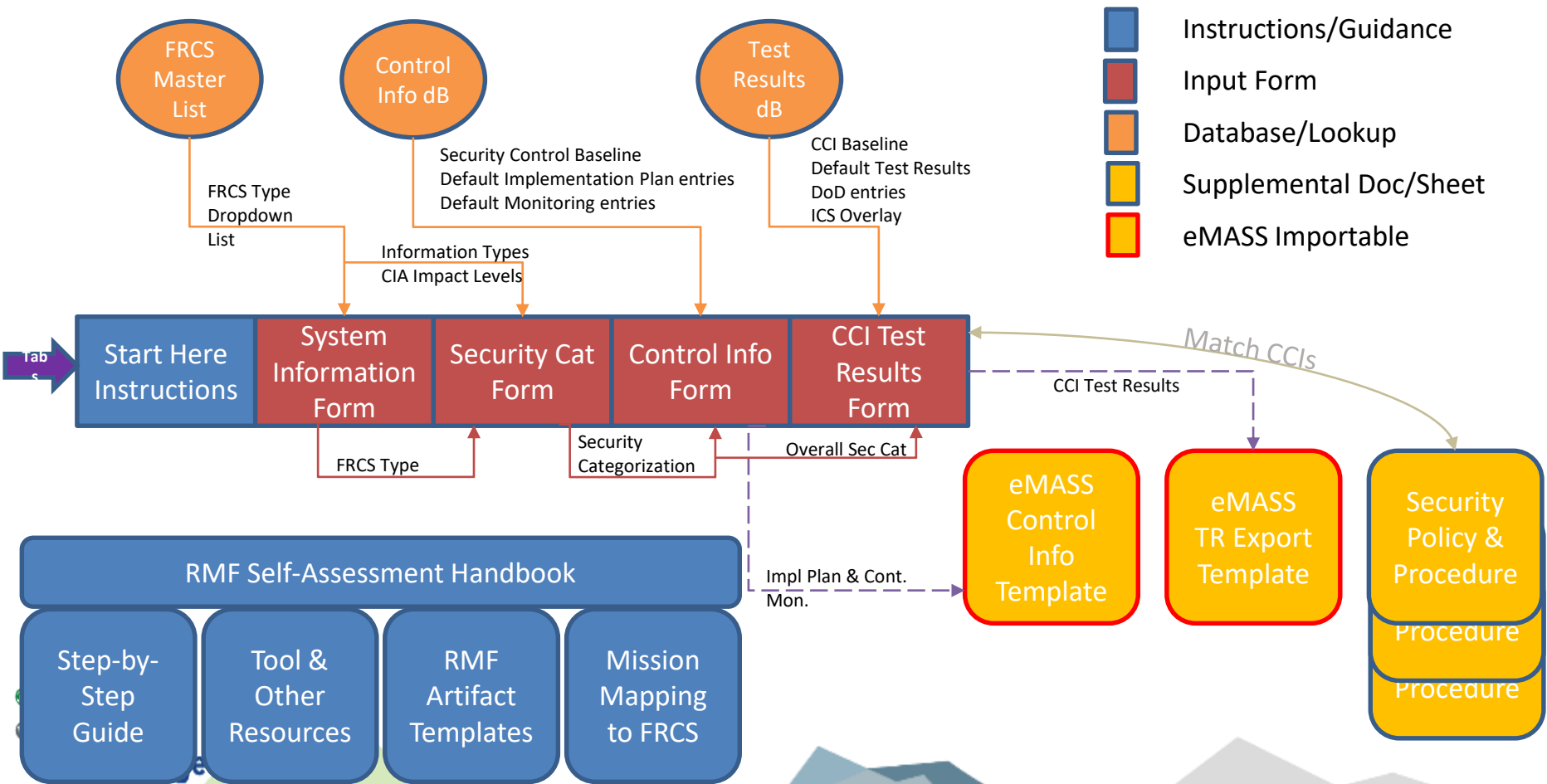
- a) Updated Draft Security Plan with security controls and CCIs determined in this step, along with other artifacts provided by the System Owner
- b) Edited guide specifications to include UFGS 25 05 11 and other specification sections with affected control systems
- c) **Cybersecurity section in the 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.
 - » 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.
- ure the OS and vendor
) are properly hardened using
is) and configured to the JIE
ce and turnover of the project
te.
- is a functional recovery point
should capture the FMC
s, remote access terminals,
a flow, and machine/device
formation should be kept
ranges are made to the
baseline is used to
conditions of the FRCS. The
he initial FMC baseline.
- ISCP and the FMC are used

ESCTP FRCS RMF Tool – Coming Soon!



ESCTP FRCS RMF Tool

Step 3
Implement Controls

CCI Test Results Form

The screenshot shows the 'Security Categorization Form' with various fields for system information, security categories, and a table for 'OVERALL SYSTEM SECURITY CATEGORY'.

NIST 800-82
800-82 ICS
Overlay

DoD-
level
Policies

UFC
4-010-
06

Test Result Import Template: Test for Moderate vs High

Control Number	Control Information	AP	AP-AP	CCI	CCI Definition	Implementation Guidance	RECOMMENDED EVIDENCE	Design period	Enter Test Results Here				Latest Test Results			
									Ass	Con	U	U	Ass	Con	U	U
AC-1	Access control: The organization restricts access to information and resources to authorized individuals, processes, and devices.	AP-1	AP-1	AC-1	The organization restricts access to information and resources to authorized individuals, processes, and devices.	The organization being implemented develops and documents an access control policy that addresses purpose, scope, roles, responsibilities, and management commitments.	1) Signed copy of access control policy that defines the purpose, scope, roles, responsibilities, management commitments, and objectives.	180	180	180	180	180	180	180	180	

eMASS
Import
of
Test
Results

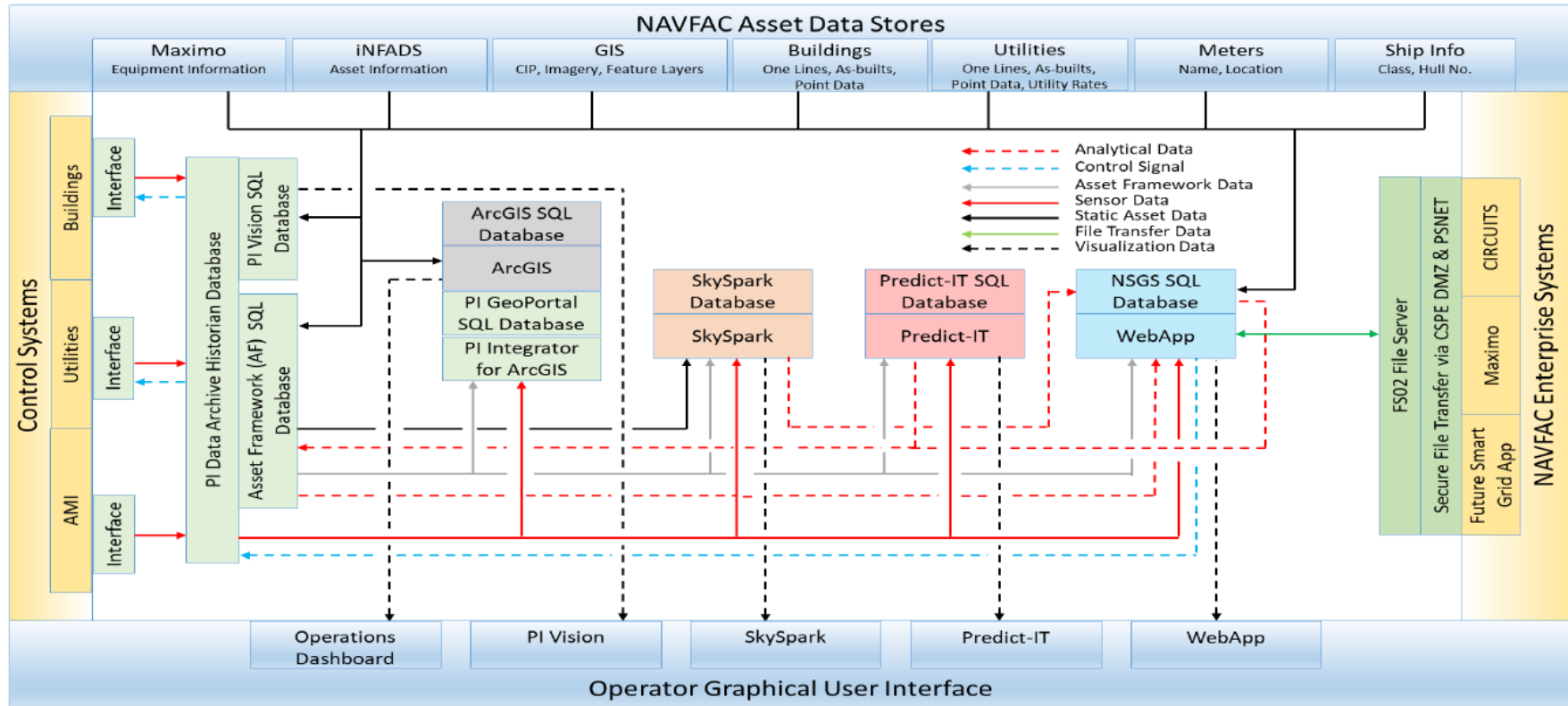
Test Result Export Form

- 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



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.**

3. How to Use These TTP

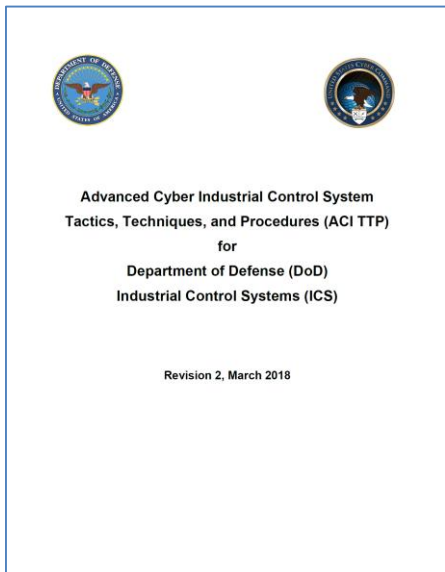
This ACI TTP is divided into essentially four sections:

- **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

Capital One Credit Cards, Bank... Industrial Control Systems (ICS)... FRCS Protecting CUI DTARS 252.204.7012 -- Bing

Capital One Credit Cards, B... USAA Login TD Ameritrade Login Wells Fargo - Banking, Cre... Welcome to LTPS online VA Taxes ShareFile - Where Compani... LinkedIn Cybersecurity WBDG Whol...

SERDP DOD • EPA • DOE | **ESTCP**

DoD's Environmental Research Programs

SEARCH

Advanced search

View All Social Media

Home About SERDP and ESTCP Program Areas News and Events Featured Initiatives Tools and Training Funding Opportunities Investigator Resources

Tools and Training

Webinar Series

Installation Energy and Water

Cybersecurity

Overview of PIT, OT & FRCS

Architecture, Networks & Components

Design and Commissioning

Test and Development Environment

Continuous Monitoring & Auditing

Registering FRCS in eMASS, DITPR, SNaP-IT

Legislation, Instructions, Manuals, Policies, Plans and Memos

Home > Tools and Training > Installation Energy and Water > Cybersecurity > FRCS Protecting CUI

FRCS Protecting CUI

Executive Order 13556 "Controlled Unclassified Information" 2010

Established by Executive Order 13556, the Controlled Unclassified Information (CUI) program standardizes the way the Executive branch handles unclassified information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies.

Controlled Unclassified Information (CUI) is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended.

Executive Order 13556 "Controlled Unclassified Information" (the Order), establishes a program for managing CUI across the Executive branch and designates the National Archives and Records Administration (NARA) as Executive Agent to implement the Order and oversee agency actions to ensure compliance. The Archivist of the United States delegated these responsibilities to the Information Security Oversight Office (ISOO).

32 CFR Part 2002 "Controlled Unclassified Information" was issued by ISOO to establish policy for agencies on designating, safeguarding, disseminating, marking, decontrolling, and disposing of CUI, self-inspection and oversight requirements, and other facets of the

PRINT

Program Areas

→ Installation Energy and Water

Featured Initiatives

→ Energy Assurance and Resilience

Share

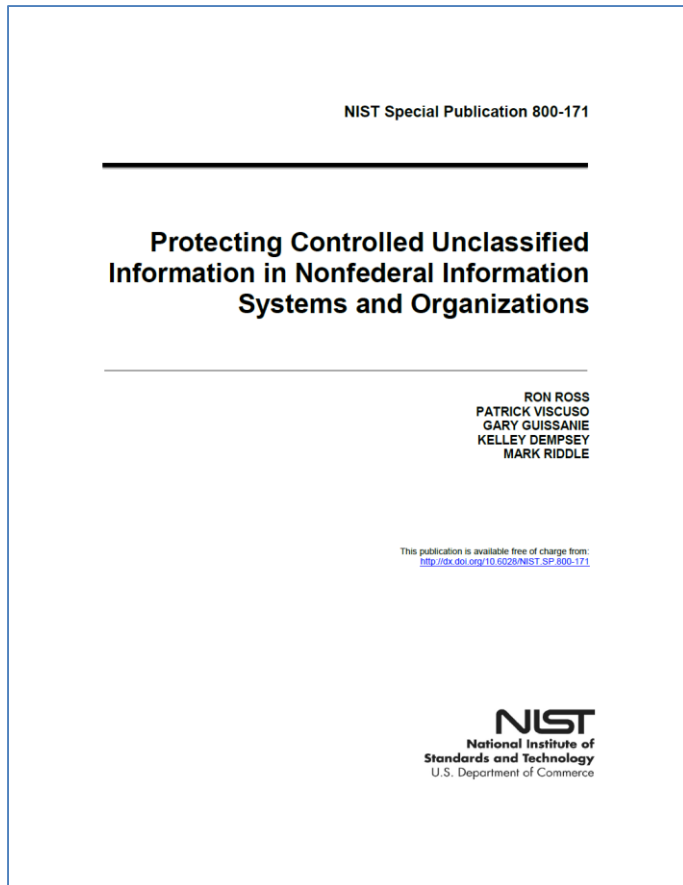
Type here to search

3:17 PM 4/5/2019

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



SUSTAINMENT

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

NOV 20 2018

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

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

UNCLASSIFIED

DoD ESCTP Cybersecurity FRCS

The screenshot shows a web browser window with the URL <https://serdp-estcp.org/Tools-and-Training/Installation-Energy-and-Water/Cybersecurity/Energy-Projects-Third-party-Financing>. The page title is "DoD's Environmental Research Programs". The navigation menu includes "Home", "About SERDP and ESTCP", "Program Areas", "News and Events", "Featured Initiatives", and "Tools and Training". The "Tools and Training" section is expanded, showing a list of items: "Webinar Series", "Installation Energy and Water", "Cybersecurity", "Overview of PIT, OT & FRCS", "Architecture, Networks & Components", "Design and Commissioning", "Test and Development Environment", "Continuous Monitoring & Auditing", "Registering FRCS in eMASS, DITPR, SNaP-IT", "Legislation, Instructions, Manuals, Policies, Plans and Memos", "Resources, Tools, and Publications", "Templates and Checklists", and "Software". The main content area displays the breadcrumb "Home > Tools and Training > Installation Energy and Water > Cybersecurity > Energy Project Third-part..." and the title "Utility Privatization Program, Energy Projects, Third-party Financing, and Cybersecurity". The text below the title states: "The DoD has special legislative and Executive Order authorization for the acquisition of energy projects. These include Energy Savings Performance Contracts (ESPCs), Utility Energy Services Contracts (UESCs), Utilities Privatization (UP), Energy Resilience and Conservation Investment Program (ERCIP), and other contract or program vehicles. Cybersecurity requirements are now contractually required for third-party energy providers to ensure that, both DoD Information Network (DoDIN) and DoD Controlled Unclassified Information (CUI) data is protected from cyber threats; and that third parties who provide energy services to DoD are able to detect, mitigate and recover from a cyber attack. Energy security, resilience and cybersecurity are foundational elements for installation mission assurance." Below this text is a section titled "FOR IMMEDIATE ACTION - Assistant Secretary of Defense for Sustainment (ASD(s)) Supplemental Guidance for the Utilities Privatization Program Memorandum Feb 7, 2019". The text in this section reads: "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 accountable for system operation resilience and cybersecurity, including the safeguarding of CDI related to utility services. Effective immediately, the DoD Components shall incorporate references (x) to (b) in all new or renewing utility service contracts, or contracts undergoing material modifications price determinations. **Additionally, no later than sixty (60) days after the issuance**

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**

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

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.

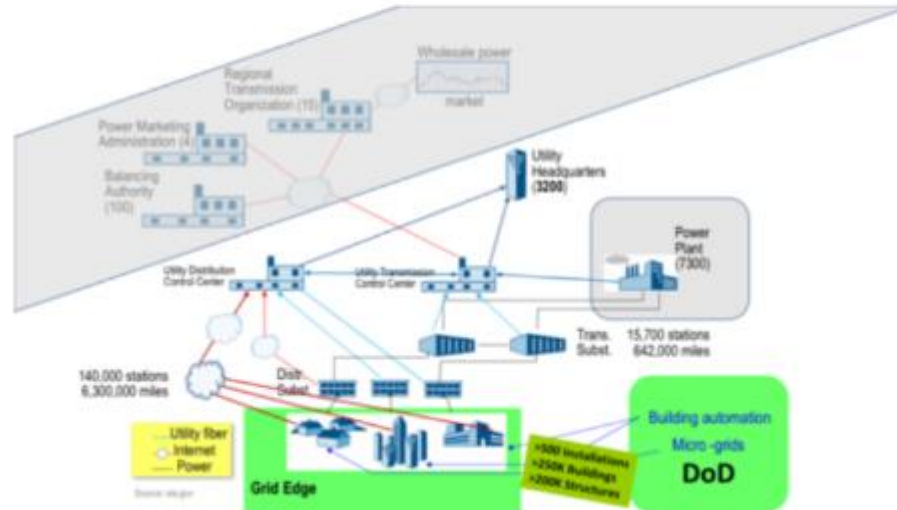


Figure 2 – DoD Energy Data Flows

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):

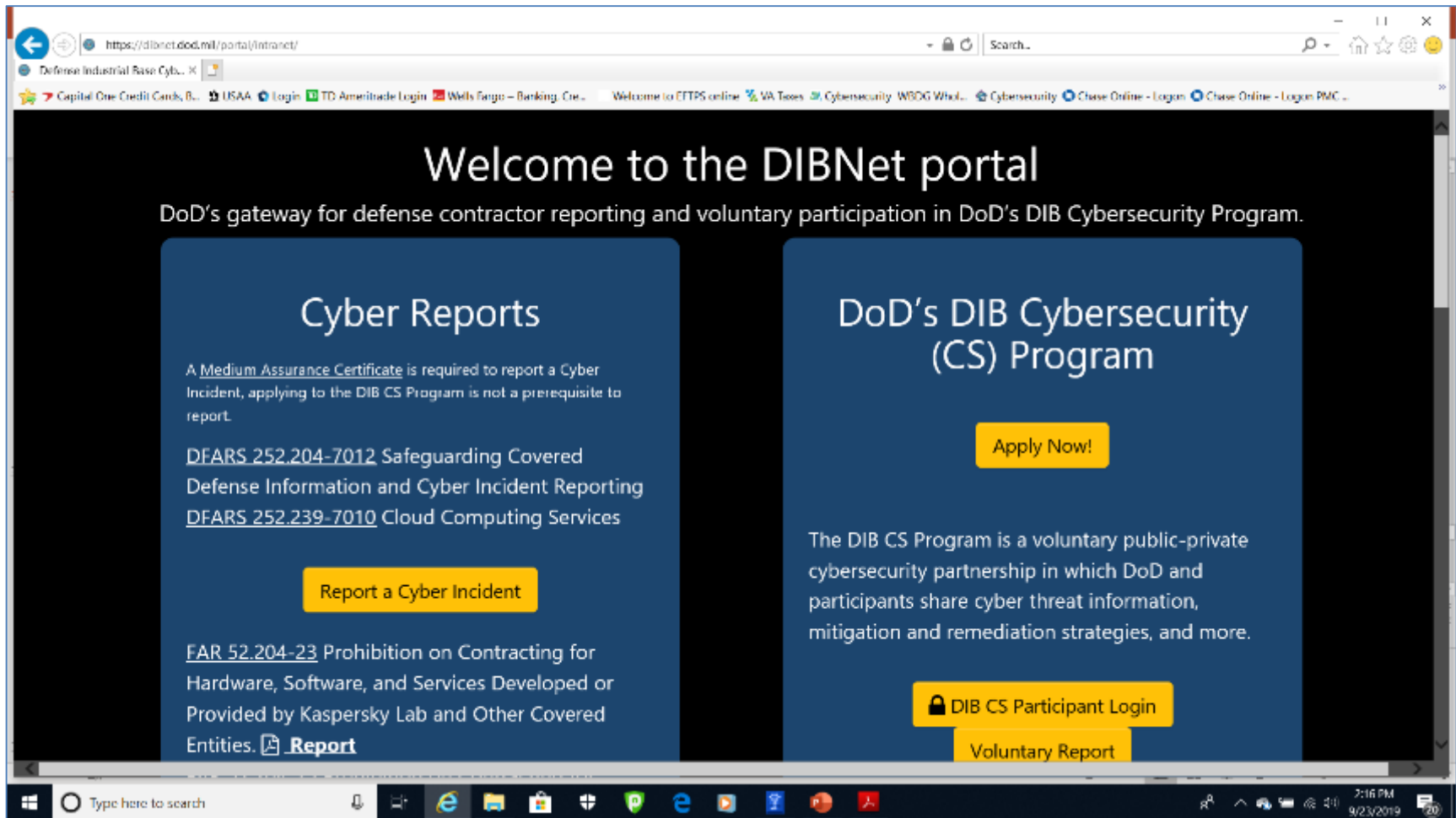
- C.2.8.12 General Information
- C.3.1.1 Facilities, Fleet, and Equipment Management Information Type
- C.3.5.8 System and Network Monitoring Information Type
- D.2.2 Key Asset and Critical Infrastructure Protection Information Type
- D.7.1 Energy Supply Information Type

Cyber Risk Plans for Business and CS

Envelopes	protected.		
Environmental Restoration			
Munitions Response			
Resource Conservation and Resiliency			
Weapons Systems and Platforms			
	<p>Cyber Risk Management Plans - NIST Standards</p> <p>Applies To FRCS Networks, Components and Devices</p> <p>Contractual Requirement UFC 04-010-06 and UFGS 25-11-05 Cybersecurity of Facility Related Control Systems</p> <p>Owned and Operated by UP Contractor UP Contractor to submit FRCS RMF Package and obtain Authority To Operate (ATO)</p> <p>Owned by DoD Operated by UP Contractor DoD to submit FRCS RMF Package and obtain Authority To Operate (ATO)</p> <p>Metric/Measure, Requirement</p> <ul style="list-style-type: none"> → All FRCS on separate segmented and secure network → All FRCS being continuously monitored (IAW Risk Management Framework (RMF) compliance Schema detailed in FRCS Cybersecurity Plan Guidance) → All FRCS registered in Enterprise Mission Assurance Support System (eMASS) or alternative equivalent repository → Plan for risk mitigation and 	<p>NIST SP 800-82</p> <p>NIST SP 800-171</p> <p>Corporate IT business systems that host or transmit CUI</p> <p>DFARS 252.204.7012 – Safeguarding Covered Defense Information and Cyber Incident Reporting</p> <p>UP Contractor to submit CUI CRMP</p> <p>UP Contractor to submit CUI CRMP</p> <ul style="list-style-type: none"> → Cyber Risk Management Plan (CRMP) or other report format of implementation of reference (y) IAW with reference (x) → 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



The screenshot shows a web browser window displaying the DIBNet portal. The address bar shows the URL <https://dibnet.dod.mil/portal/intranet/>. The page features a dark blue background with white text. At the top, it says "Welcome to the DIBNet portal" and "DoD's gateway for defense contractor reporting and voluntary participation in DoD's DIB Cybersecurity Program." Below this, there are two main sections. The left section is titled "Cyber Reports" and includes text about the Medium Assurance Certificate requirement, links to DFARS 252.204-7012 and DFARS 252.239-7010, and a yellow button labeled "Report a Cyber Incident". The right section is titled "DoD's DIB Cybersecurity (CS) Program" and includes a yellow button labeled "Apply Now!". Below this, there is text describing the program as a voluntary public-private partnership, and a yellow button labeled "DIB CS Participant Login" with a sub-button labeled "Voluntary Report". The browser's taskbar at the bottom shows various application icons and the system clock indicating 2:16 PM on 9/23/2019.

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

Welcome to the DIBNet portal
DoD's gateway for defense contractor reporting and voluntary participation in DoD's DIB Cybersecurity Program.

Cyber Reports

A Medium Assurance Certificate is required to report a Cyber Incident, applying to the DIB CS Program is not a prerequisite to report.

[DFARS 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting](#)
[DFARS 252.239-7010 Cloud Computing Services](#)

[Report a Cyber Incident](#)

[FAR 52.204-23 Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities.](#) [Report](#)

DoD's DIB Cybersecurity (CS) Program

[Apply Now!](#)

The DIB CS Program is a voluntary public-private cybersecurity partnership in which DoD and participants share cyber threat information, mitigation and remediation strategies, and more.

[DIB CS Participant Login](#)
[Voluntary Report](#)

<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 [portal](#)⁴. *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.**

Cybersecurity Maturity Model Certification

	Description of Practices	Description of Processes
Level 1	<ul style="list-style-type: none"> • Basic cybersecurity • Achievable for small companies • Subset of universally accepted common practices • Limited resistance against data exfiltration • Limited resilience against malicious actions 	<ul style="list-style-type: none"> • Practices are performed, at least in an ad-hoc matter
Level 2	<ul style="list-style-type: none"> • Inclusive of universally accepted cyber security best practices • Resilient against unskilled threat actors • Minor resistance against data exfiltration • Minor resilience against malicious actions 	<ul style="list-style-type: none"> • Practices are documented
Level 3	<ul style="list-style-type: none"> • Coverage of all NIST SP 800-171 rev 1 controls • Additional practices beyond the scope of CUI protection • Resilient against moderately skilled threat actors • Moderate resistance against data exfiltration • Moderate resilience against malicious actions • Comprehensive knowledge of cyber assets 	<ul style="list-style-type: none"> • Processes are maintained and followed
Level 4	<ul style="list-style-type: none"> • Advanced and sophisticated cybersecurity practices • Resilient against advanced threat actors • Defensive responses approach machine speed • Increased resistance against and detection of data exfiltration • Complete and continuous knowledge of cyber assets 	<ul style="list-style-type: none"> • Processes are periodically reviewed, properly resourced, and improved across the enterprise
Level 5	<ul style="list-style-type: none"> • Highly advanced cybersecurity practices • Reserved for the most critical systems • Resilient against the most-advanced threat actors • Defensive responses performed at machine speed • Machine performed analytics and defensive actions • Resistant against, and detection of, data exfiltration • Autonomous knowledge of cyber assets 	<ul style="list-style-type: none"> • 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

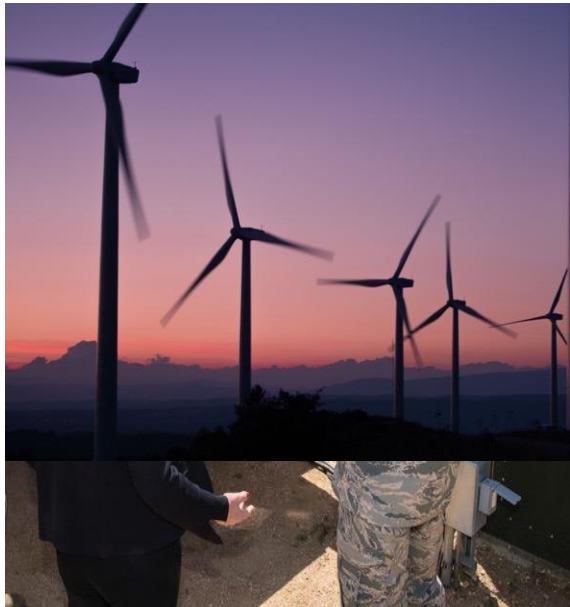


EPIR Webinar

14 Nov 2019

Military Energy Resilience Catalyst (MERC)

Regional Identification of Gaps for Operational Resilience (RIGOR)



AGENDA AND OVERVIEW

- Converge Strategies Overview
- Military Energy Resilience Catalyst
- Regional Identification of Gaps for Operational Resilience

CONVERGE STRATEGIES



CONVERGE
STRATEGIES

**EXPANDS ENERGY INNOVATION
TO KEEP AMERICA SECURE**

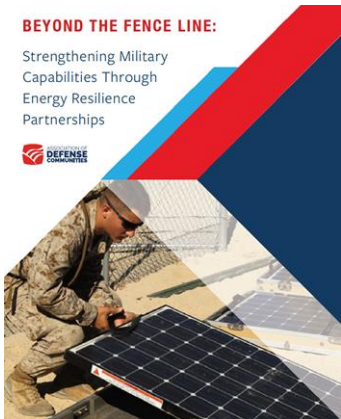
DEPARTMENT OF DEFENSE
ENERGY RESILIENCE

CIVILIAN-MILITARY
PARTNERSHIPS

HOMELAND SECURITY AND ADVANCED
ENERGY

BEYOND THE FENCE LINE:

Strengthening Military
Capabilities Through
Energy Resilience
Partnerships



MILITARY
ENERGY
RESILIENCE
CATALYST

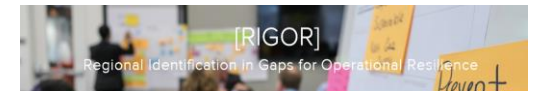


NARUC
National Association of Regulatory Utility Commissioners

The Value of Resilience for Distributed Energy Resources:
An Overview of Current Analytical Practices



Prepared for The National Association of Regulatory Utility Commissioners
Prepared by Converge Strategies, LLC
April 2019



[RIGOR]

Regional Identification in Gaps for Operational Resilience

The Problem

Over 95% of DoD installations rely on the civilian electric grid for power. Military installations and defense communities share regional infrastructure systems, like water and electricity. These lifeline systems are interdependent and increasingly threatened by determined adversaries and environmental impacts, endangering mission assurance.

The Solution

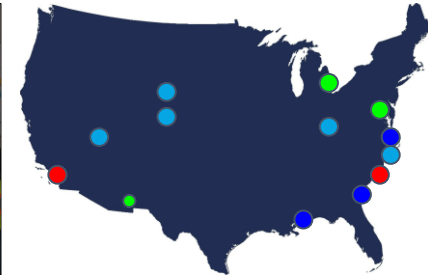
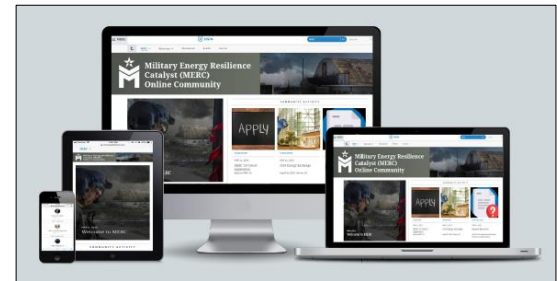
RIGOR strengthens the resilience of DoD installations and defense communities. Converge Strategies and Idaho National Laboratory (INL) will convene DoD installation leadership and lifeline infrastructure owners to develop an understanding of cross-sector interdependencies. These teams will identify and develop project concepts and implementation plans to strengthen the resilience of DoD installations and defense communities.



MILITARY ENERGY RESILIENCE CATALYST [MERC]

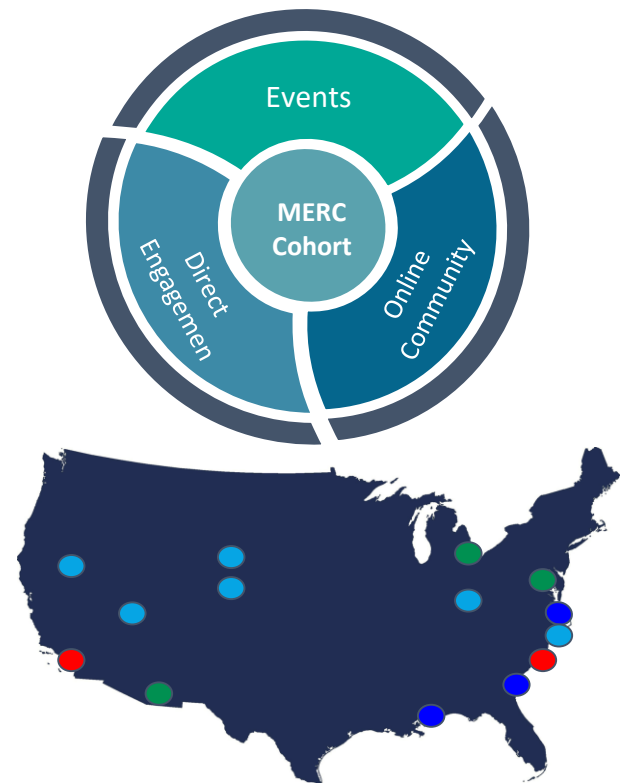
MERC is an accelerator program for DoD energy resilience professionals

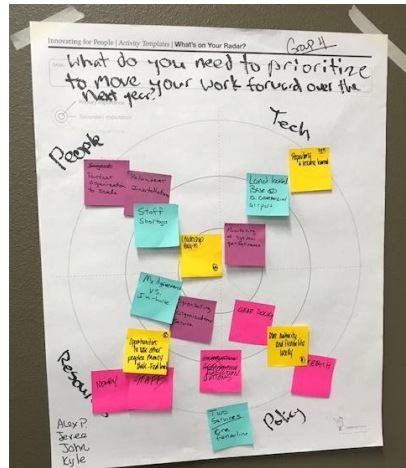
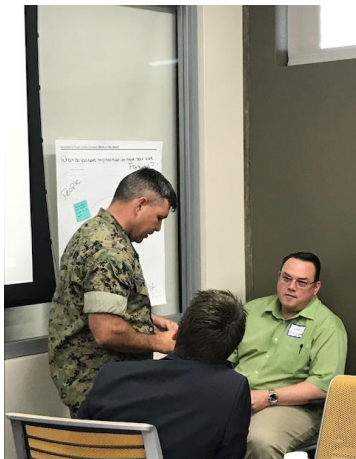
- Funded through the DoD Environmental Security Technology Certification Program (ESTCP), DoD's test-bed program
- Brings together experts and practitioners from across DoD and the energy world to strengthen DoD energy resilience efforts and overcome barriers to project development
- The MERC program is composed of three pillars: Online Community, Peer-to-Peer Network, and Installation Workshops



Sixteen DoD energy resilience professionals nominated by service energy leads based on their leadership at installations across the country.

- Core of MERC's strategy to accelerate DoD energy resilience development
- Supported by MERC Faculty guidance, connections, and educational materials
- Three TDY trips focused on advancing energy resilience projects and policies specific to each cohort member
- ESTCP program supports technology transition to the installations of the cohort members.





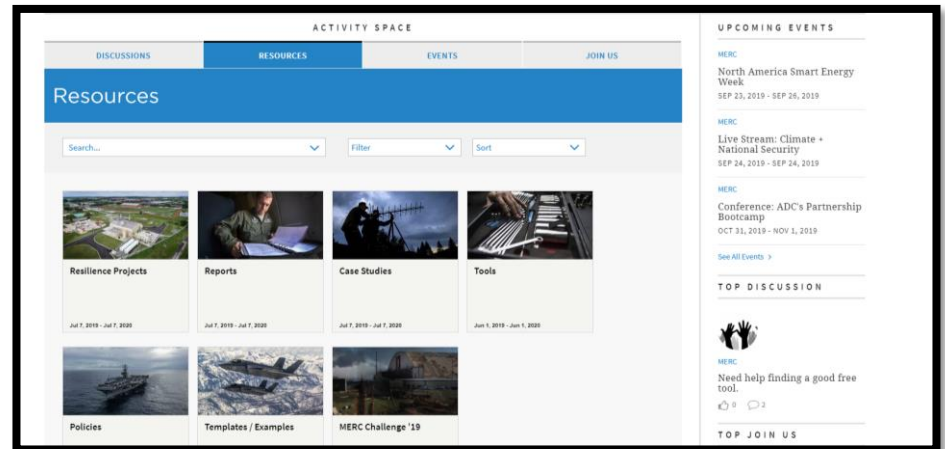
“I have access to people who have done this before so I don’t have to recreate the wheel” – Brian O’Leary, Peterson AFB

“This is an example of the [DoD] organization really funding [its] people” – Mick Wasco, MCAS Miramar

“I can go back to leadership and report to them what people at the installation want” – MERC Faculty Member

“We don’t have to exist in silos. Having access to policy makers to help me push through and navigate hurdles is invaluable” – Shannon Bergt, Detroit Arsenal

MERC ONLINE COMMUNITY



<https://innovatedefense.net/merc>

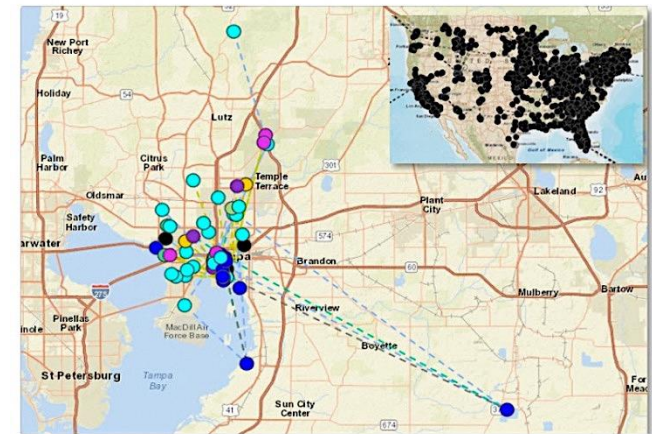
The MERC Online Community was launched at Energy Exchange!

- Resource hub of tools and templates
- Forthcoming database of completed, ongoing, and planned projects, searchable by key attributes w/ POCs for P2P matchmaking
- Online interactions, upcoming events, challenges, and more!

Regional Identification of Gaps for Operational Resilience

- **The Problem:** Military installations and defense communities share regional infrastructure systems, like water, gas, and electricity. These lifeline systems are interdependent and increasingly threatened by adversaries and extreme weather.
- **The Solution:** Converge Strategies and the Idaho National Laboratory convene regional stakeholders to understand the cross-sector interdependencies. The teams apply the All Hazard Analysis tool to map critical community and installation assets, identify interdependencies to help identify and develop project concepts to strengthen DoD installations.

The All Hazard Analysis (AHA) Tool



Regional Identification of Gaps for Operational Resilience

The RIGOR process is designed to bring regional critical infrastructure and asset owners and stakeholders together with Federal (DoD, DOE, and DHS), State, and Local government officials to collaboratively address installation resilience and interdependencies.

Improve Installation Resilience: The RIGOR process identifies regional resilience challenges, infrastructure interdependencies, and impacts to support multi-stakeholder project identification and development.

Demonstrate leadership and progress on Federal and DoD Policies:

DoD Community Resilience Policies	RIGOR Impact
Presidential Policy Directive 21 identifies the lifeline sectors that, if disabled, would be debilitating.	RIGOR focuses on these lifeline sectors to identify vulnerabilities that would impact the ability of the installation to continue to execute its critical missions.
OSD Mission Assurance is creating channels to enable information sharing between DoD, utility providers and infrastructure owners on critical assets, and requirements.	RIGOR convenes these stakeholders in a setting that enables the sharing of current and future vulnerabilities and allows for project development to address large scale issues.
OSD Sustainment is developing comprehensive policy that requires installations to conduct resilience workshops, evaluations, and exercises.	RIGOR supports these requirements and identifies additional stakeholders and partners for project funding and vulnerabilities outside the fence line.

Regional Identification of Gaps for Operational Resilience (RIGOR) – Anchorage Workshop

Project Concepts: Participants identified actionable resilience project concepts, developed detailed action plans, and identified required key stakeholders for success



Process for prioritizing micro-grid development at targeted essential function locations to ensure operations during macro grid failure. (Alaska Partnership for Infrastructure Protection)



Novel locomotive/solar + storage power backup project at the Port of Alaska to ensure continuity of operations. (Port of Alaska, JBER, DOE, Ted Stevens International Airport)



Stakeholder engagement approach to develop technical solutions to ensure uninterrupted natural gas supply. (ENSTAR, Electric Utilities)



New Anchorage cross-town natural gas routing/looping capabilities to increase resilience in the event of disruption. (ENSTAR, Muni, Electric Utilities, JBER)



Expand State of Alaska owned and operated Alaska Land Mobile Radio (ALMR) system to allow private critical asset owner access for statewide emergency communications. (ACS, GCI, JBER)

Success

- Department of Energy – Office of Electricity has funded a feasibility study on the Port project
- Engagement from ENSTAR continues for resilience projects supporting the city and installation
- DHS/DOE continue to invest in Anchorage, using RIGOR projects and launching point

Emerging Resources for Energy Resilience Planning

Program	Overview	Eligibility and Potential Use
Office of Economic Adjustment (OEA) Installation Resilience	2019 NDAA authorizes grants, cooperative agreements, and supplemental funds to address “threats to military resilience”	States, counties, communities surrounding or supporting DoD installations. Could include off-base energy infrastructure protection. Focused on funding approaches, studies, evaluations.
OEA Compatible Use / REPI Authority	2019 NDAA Authority for REPI to “maintain or improve military installation resilience” Provides funding to promote activities that support the continued operational utility of a military installation.	Focused on nature-based encroachment barriers, infrastructure projects(e.g. solar PV facilities) that protect the environment around installations Joint Land Use Study, State or local government proposal to promote compatible siting of energy projects to prevent adverse impacts to DoD.
Defense Community Infrastructure Program (DCIP)	2019 NDAA authorizes DCIP funds to support off-base energy infrastructure that can further DoD mission assurance and energy resilience objectives.	Communities that support DoD installations. Interest in mission support driven projects with buy-in from Installation Commanders.