OSD's Energy Technology Demonstration Program

Environmental Security Technology Certification Program (ESTCP)

Tim Tetreault, ESTCP Program Manager
Dr. Mike Chipley, PMC Group – Cybersecurity Consultant

November 9, 2021

Outline

- SERDP-ESTCP Overview
- Installation Energy and Water (EW) Program Area
- Active Projects
- Cybersecurity Process and Resources

DoD's Environmental & Energy Technology Programs

Strategic Environmental Research and Development Program

SCIENCE AND TECHNOLOGY

- Fundamental research to impact DoD environmental land management
- Advanced technology development to address near-term needs

Environmental Security Technology Certification Program

DEMONSTRATION/VALIDATION

- Innovative cost-effective environmental and energy technology demonstrations
- Promote technology implementation by direct insertion and partnering with end users and regulators

Program Area Management Structure

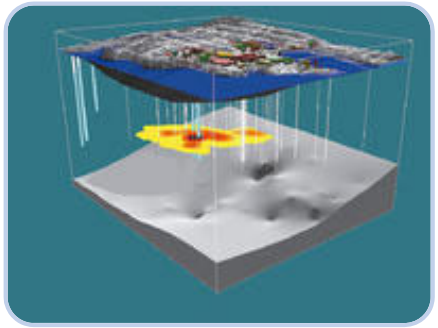
COMMON REQUIREMENTS AND SCHEDULE

Installation Energy & Water

Munitions Response

Resource Conservation & Resiliency

Environmental Restoration



Weapons Systems & Platforms

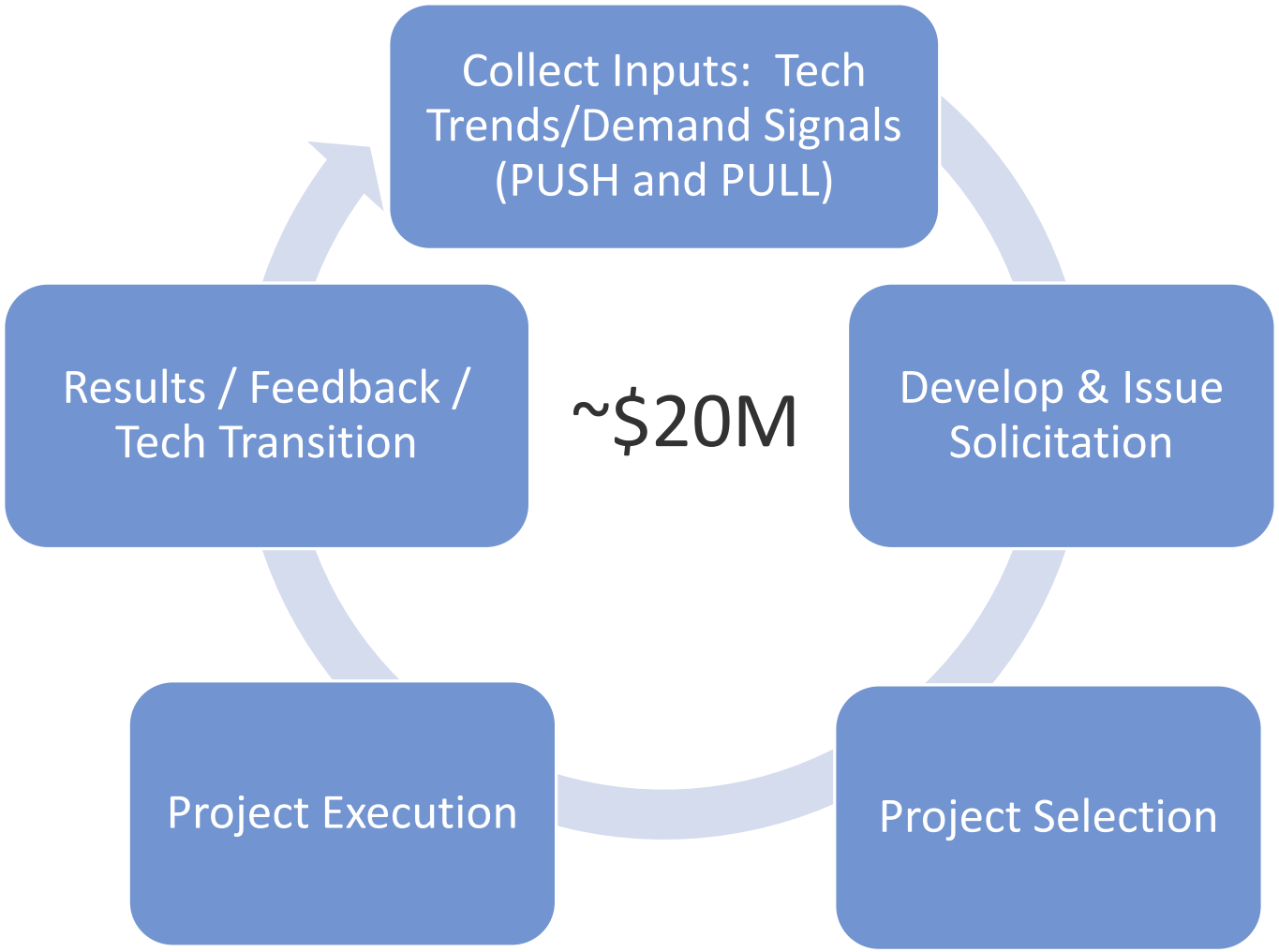
CENTRALIZED MANAGEMENT AND COORDINATION

ESTCP Installation Energy and Water (EW) Program Area Mission Statement

Advance and sustain DoD installation mission capabilities by:

- ***Identifying high impact technologies***
  that can improve DoD EW efficiency and resilience,
- ***Contributing to the body of knowledge***
  that informs energy and water tech investments, and
- ***Enabling accelerated transfer and deployment***
  of proven technologies across DoD.

Process and Participants



Technical Committee

Air Force (AFCEC)

Army (HQDA, USACE-CERL,

Navy (NAVFAC, EXWC)

OSD (ODASD-Energy)

DOE (BTO, ARPA-E, FEMP)

GSA (GPG)

EPA

MIT-LL

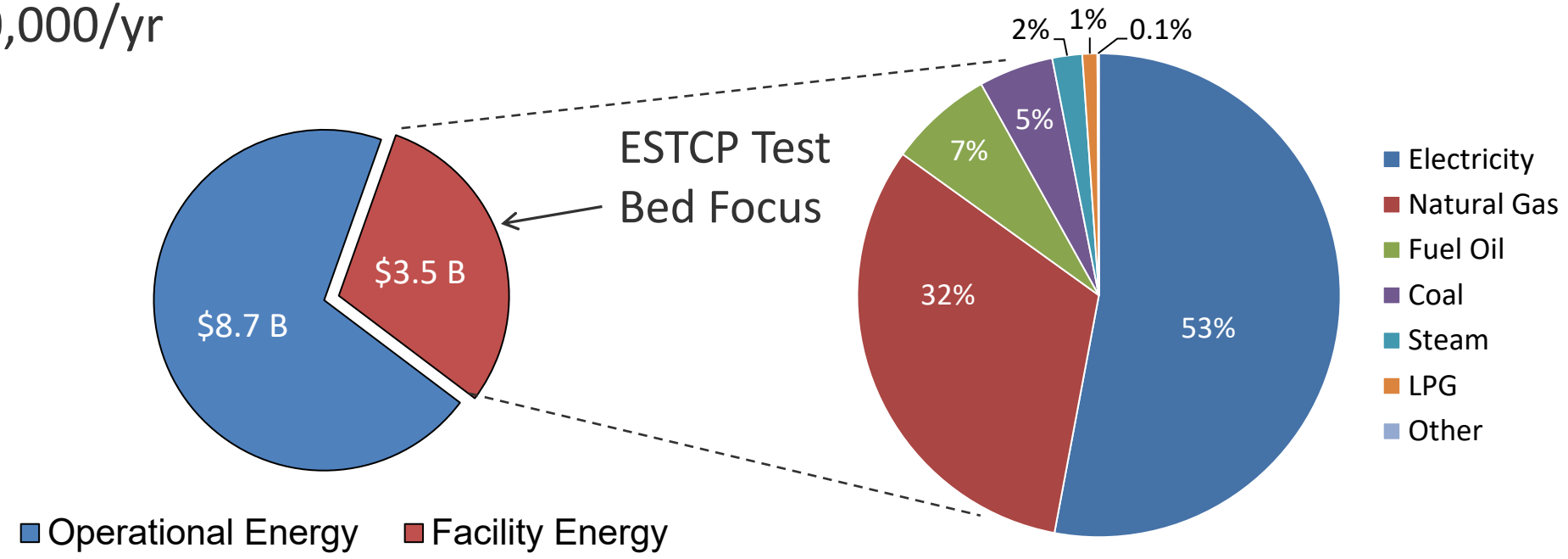
Technical Advisors

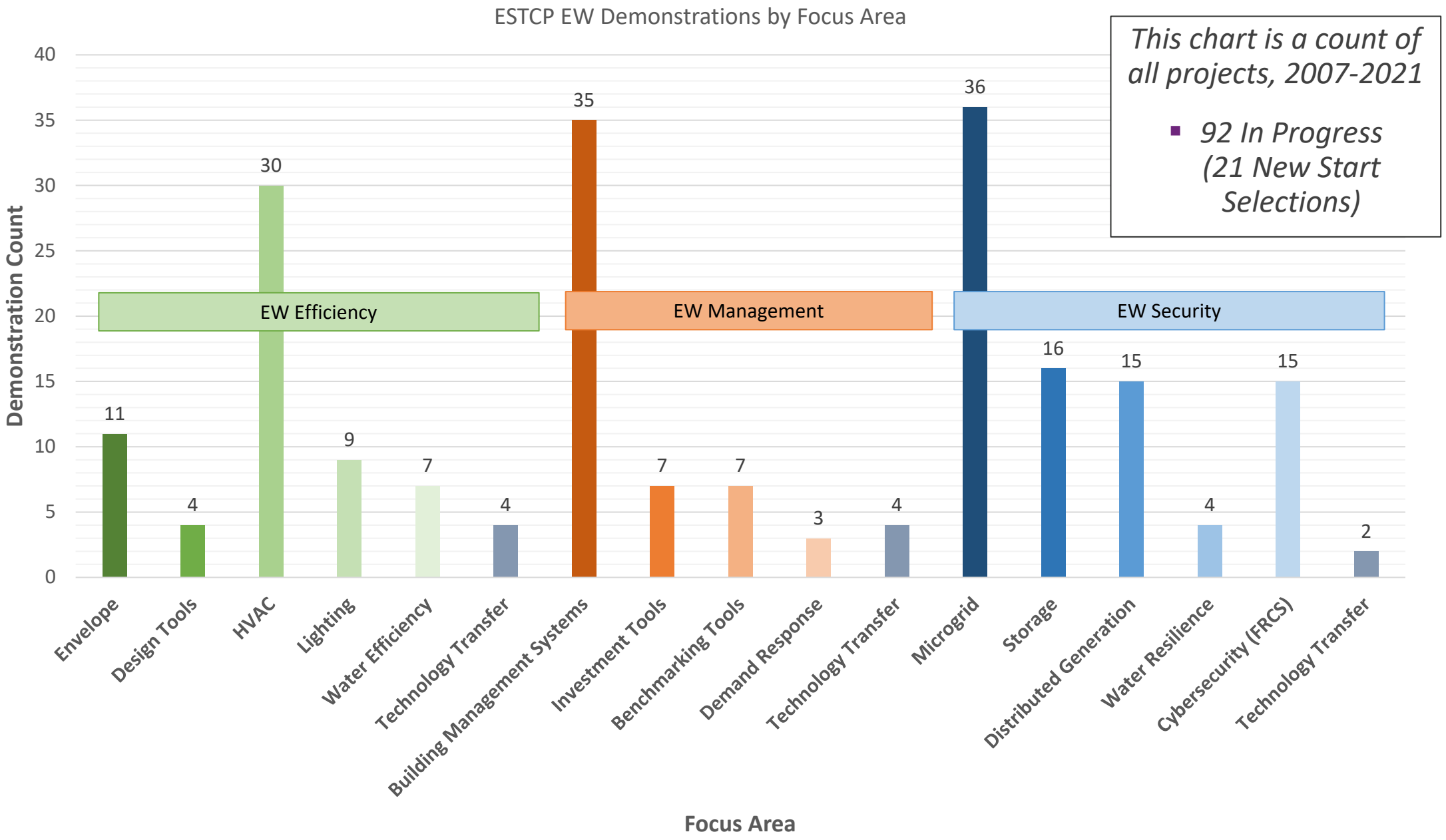
DOE Labs (NREL, LBNL, PNNL)

Private Consultants (Cyber)

Installations – Infrastructure and Energy

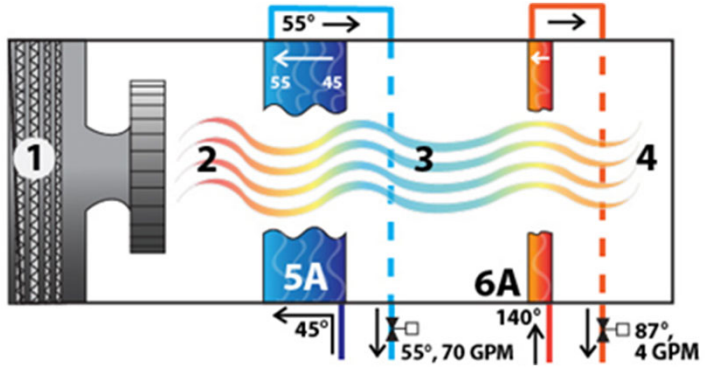
- 500 Installations
- 300,000 facilities - buildings, utilities, runways etc.
- 200,000,000 MBtus/yr
- $3,500,000,000/yr



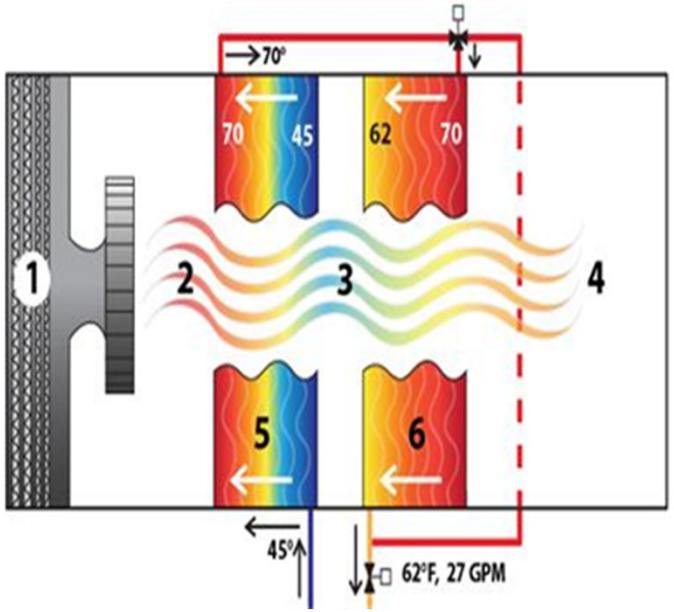

ESTCP EW Demonstrations by Focus Area
This chart is a count of all projects, 2007-2021
92 In Progress (21 New Start Selections)
Demonstration Count
Focus Area
EW Efficiency
EW Management
EW Security
Envelope
Design Tools
HVAC
Lighting
Water Efficiency
Technology Transfer
Building Management Systems
Investment Tools
Benchmarking Tools
Demand Response
Technology Transfer
Microgrid
Storage
Distributed Generation
Water Resilience
Cybersecurity (FRCS)
Technology Transfer
11
4
30
9
7
4
35
7
7
3
4
36
16
15
4
15
2

EW-201344: High Efficiency Dehumidification System (HEDS)

Traditional AHU – Dehumidification/Reheat



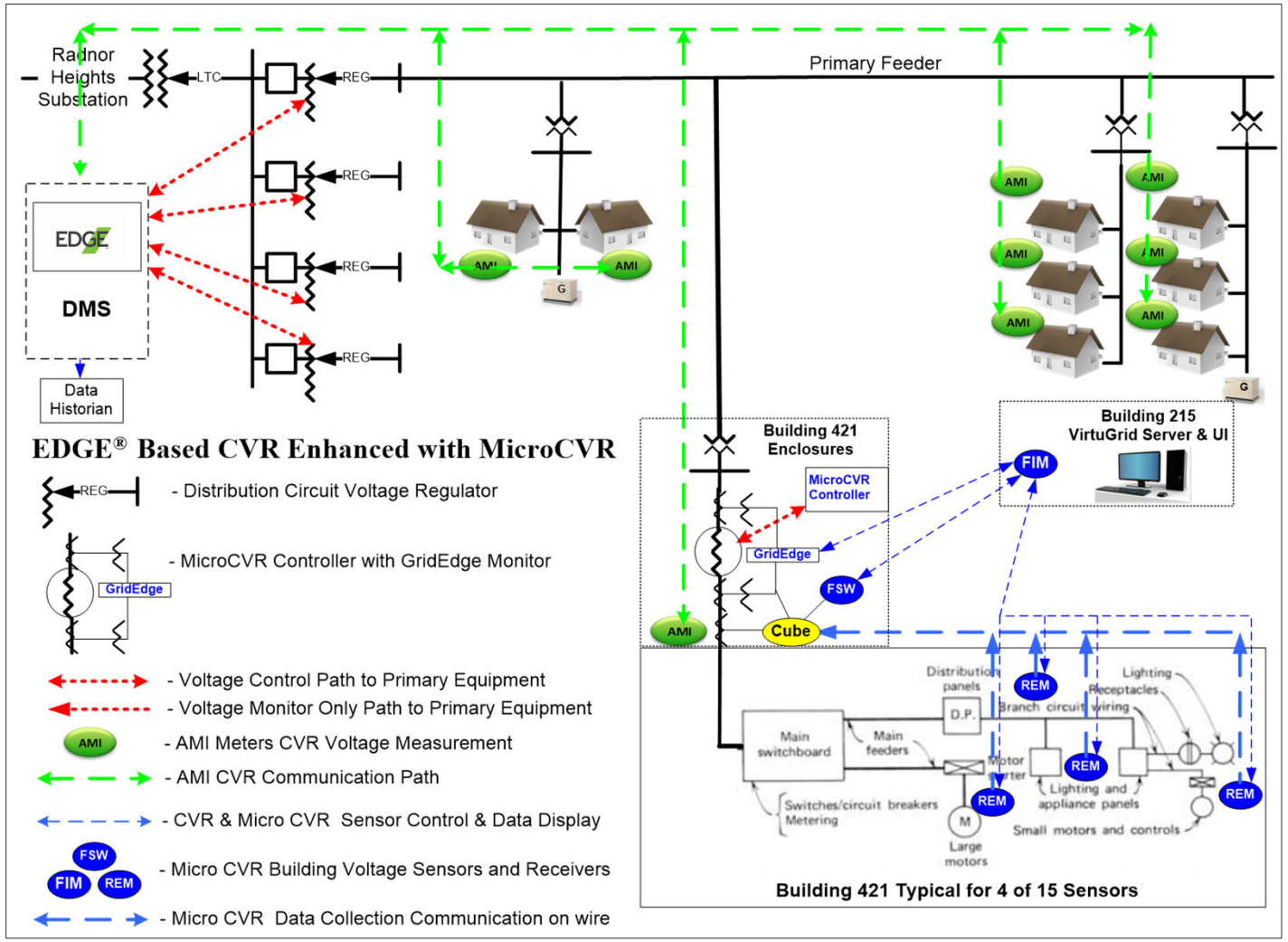
High Efficiency Dehumidification System (HEDS)



- **Technology**: The HEDS technology is very simple, comprised of a standard AHU with two deep, low face velocity heat transfer coils: a cooling coil and a cooling recovery coil. The first coil does the cooling and dehumidifying, the second coil uses the warm water leaving the cooling coil and does the reheating for RH control and cuts the loads on the chiller and boiler plants.
- **Demonstration Results**:
  - Cooling load savings are relative to incumbent systems and ranged from 20% to 30%
  - Relative humidity control was improved
  - Simple design reduces maintenance burden
  - Larger coils require more space than traditional design
  - Follow-on projects to facilitate technology transition
- **Demonstration Site:**
  - Fort Bragg, NC
  - Tinker AFB, OK
- **Performers**:
  - Datzhen Chu (USACE-CERL), Scot Duncan (Conservant Technologies)

EW-201519: Utilization of Advanced Conservation Voltage Reduction (CVR) for Energy Reduction on DoD Installations

- **Technology**: CVR is an automated system-level voltage reduction technology that optimizes voltage to continuously reduce energy consumption. MicroCVR applies the same electrical principles at the building-level to improve performance by using high-speed voltage regulation and appliance level monitoring.
- **Results**:
  - 3.7% site-wide electrical energy savings over the 12 month demonstration period.
  - 5% building-level energy savings for specific loads. MicroCVR results depend heavily on the size and type of building loads.
- **Demonstration Site**:
  - Joint Base Myer-Henderson Hall, VA
- **Performers**:
  - Brandon Stites, Dominion Power



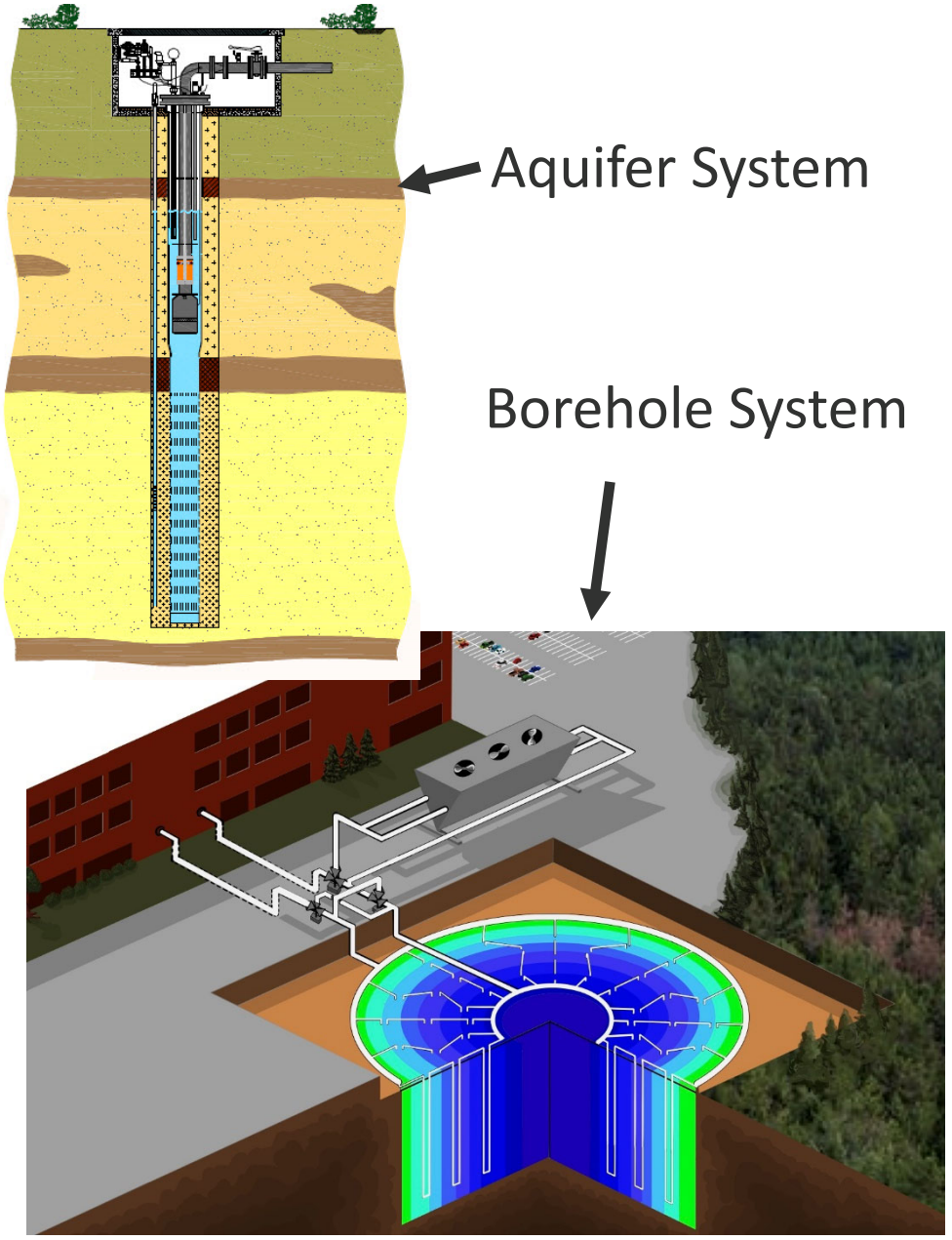
EW-201135, 18-5311: Geothermal Heat Pumps with Underground Thermal Energy Storage (UTES)

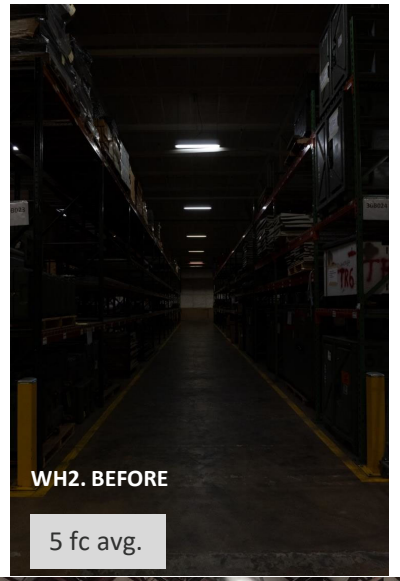
- **Technology**: Utilizes ground water or geology to serve as the building's heat source, heat sink, and underground thermal storage system to capture the building's own waste heat and waste cold to efficiently heat and cool the building in the respective season.

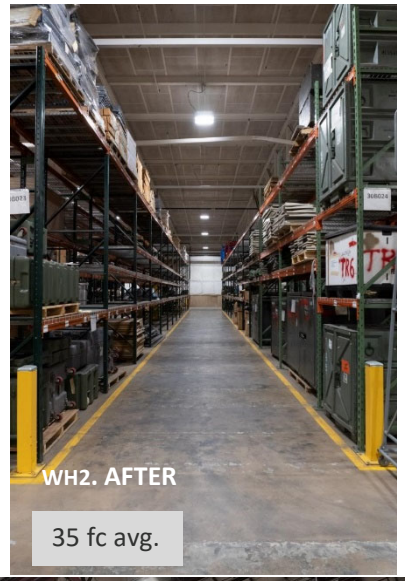
- **Performance Objectives**:
  - Reduce building's HVAC energy consumption by 40-50% .
  - Reduce building HVAC water consumption by 80-100%.
  - Eliminate on-site carbon emissions associated with water heating.

- **Demonstration Sites**:
  - MCLB Albany, GA
  - Fort Benning, GA
  - Pensacola Naval Air Station (pending)
  - Joint Base Langley Eustis (pending)

- **Performers**:
  - Chuck Hammock | Andrews, Hammock, and Powell
  - Eric Myers | Gulf Power Company
  - Chuck Hammock | Andrews, Hammock, and Powell







Dimmest spot under wing is brighter than brightest spot in empty hangar with original lights

EW-201718: Validating the Digital Lumens LED Lighting Control Retrofit

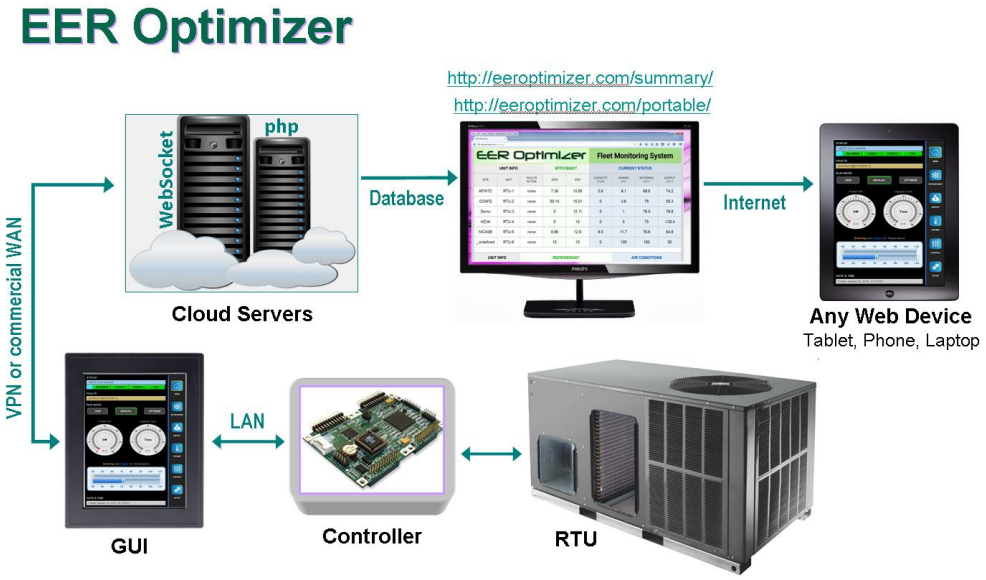
- **Technology**: Automated LED lighting retrofit system in a variety of DoD building types. Digital Lumens Intelligent Lighting System uses wireless communication to control lights. Test will validate Connected Light Engine for high-bay applications and Linear Light Engine for linear fluorescent tube retrofits.

- **Project Results**:
  - 55% lighting energy savings vs. as-found (underlit)
  - 85% lighting energy savings vs. properly-lit
  - Simple payback under 5-years
  - Fixture install time of 15-minutes
  - Lighting levels meet ANSI/ASHRAE standards.
  - Demonstrated resilient operation – fail-safe.

- **Demonstration Site:**
  - Westover Air Reserve Base, MA

- **Performers**:
  - Bryan Urban | Fraunhofer USA, Inc.

EW-201717: Next Generation Advanced High Efficiency DX Air-Conditioner Demonstration



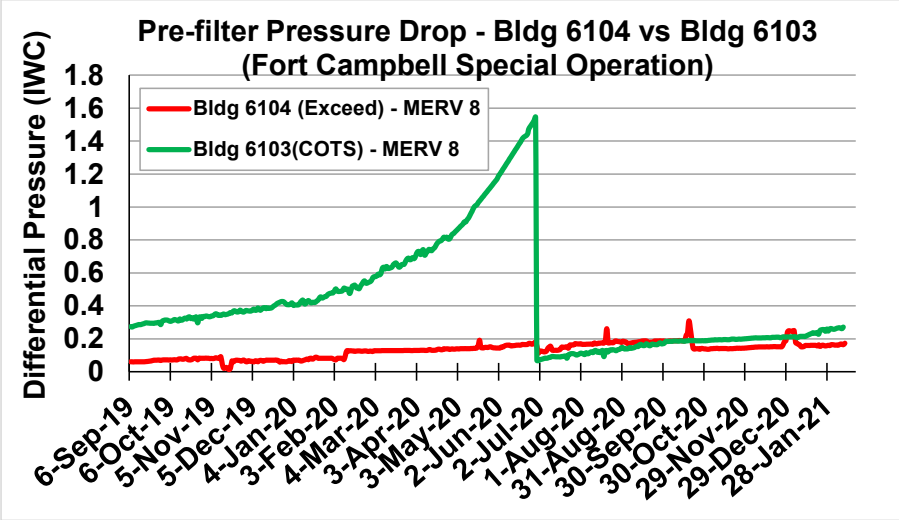
- **Technology**: Features performance optimization including: control of airflow and refrigerant level and flow, remote fault detection and diagnostics, independent control of sensible cooling and dehumidification, and remote monitoring.

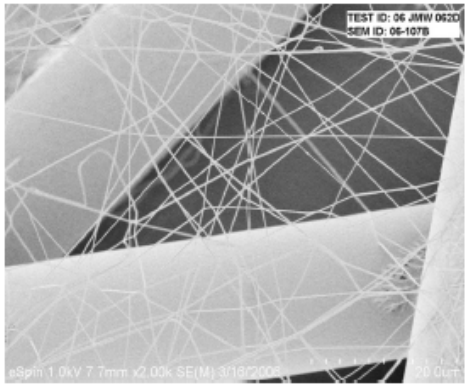
- **Demonstration Results**:
  - 45% improved efficiency over new EER 12.5 unit.
  - Fort Irwin site: 64% reduction in HVAC energy use.
  - Cape Canaveral site: 48% reduction in cooling energy use.
  - Improved dehumidification capability over standard unit.
  - Simple payback 4-8 yrs

- **Demonstration Site:**
  - Fort Irwin, CA
  - Cape Canaveral Air Force Station, FL

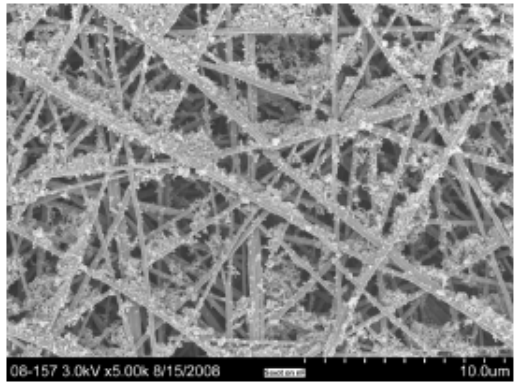
- **Performers**:
  - Michael West| Advantek Consulting

EW-201724: Nanofiber-Based Low Energy Consuming HVAC Air Filters





Nanofiber medium
Scale: 1 in ~ 20 micrometers



Weld Dust on nanofiber

- **Technology**: Nano-enabled HVAC air filtration systems to reduce energy consumption and operational cost of heating, cooling, and air purification in buildings. The filter uses small-diameter nanofiber structure with small interstitial spaces to capture contaminants.

- **Demonstration Results**:
  - 40%-70% reduction in O&M costs
    - 3x-4x longer lasting.
  - Maintain occupant comfort and indoor environment quality
  - 15-30% reduction in fan energy.

- **Demonstration Site:**
  - Arnold Air Force Base, TN
  - Redstone Arsenal, AL
  - Fort Campbell, TN
  - Fort Benning, GA

- **Performers**:
  - Jayesh Doshi | eSpin Technologies, Inc.

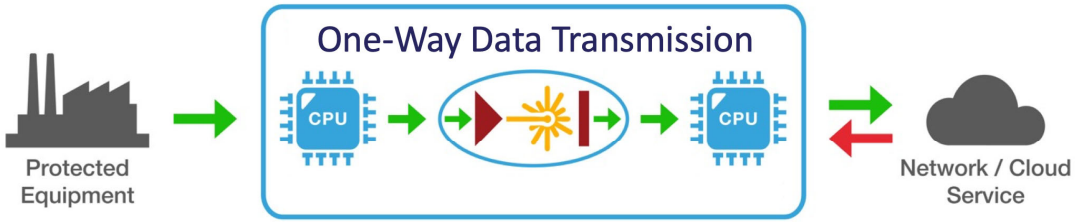
EW19-5156: Low-Cost, Plug-and-Play Data Diodes for Protection and Monitoring of DoD Facility Equipment

- **Technology**: Low-cost data diode cybersecurity hardware that extracts data from a control network or building automation system and transmits it in a physically-enforced, one-way manner to remote SCADA systems or monitoring platform for improved operational awareness.

- **Performance Objectives**:
  - Determine compatibility with DoD building equipment portfolio.
  - Measure reliability and accuracy of data transmission
  - Demonstrate ability to block inbound cyberattacks.
  - Meet cost target of <$5,000/unit

- **Demonstration Site**:
  - Performance tests: USACE ERDC-CERL, Champaign, IL
  - Penetration tests: Army Threat Systems Management Office (TSMO), Redstone Arsenal and Navy Control system Testbed.

- **Performers**:
  - Colin Dunn | Fend Incorporated
  - Tapan Patel | CERL



Unidirectional, physics-based data transfer

EW18-5333: Building Automation System Enumeration and Configuration (BASEC)

- **Technology**: BASEC protects organizations by providing scalable means to identify, baseline, and certify the cyber security configuration for building automation systems.

- **Demonstration Results**:
  - 90% coverage of BAS vendor devices.
  - 99% accurately parsed by analysis engine
  - 99% accurately identified findings.
  - >75% reduction in labor hours.
  - Follow-on project to demonstrate continuous monitoring

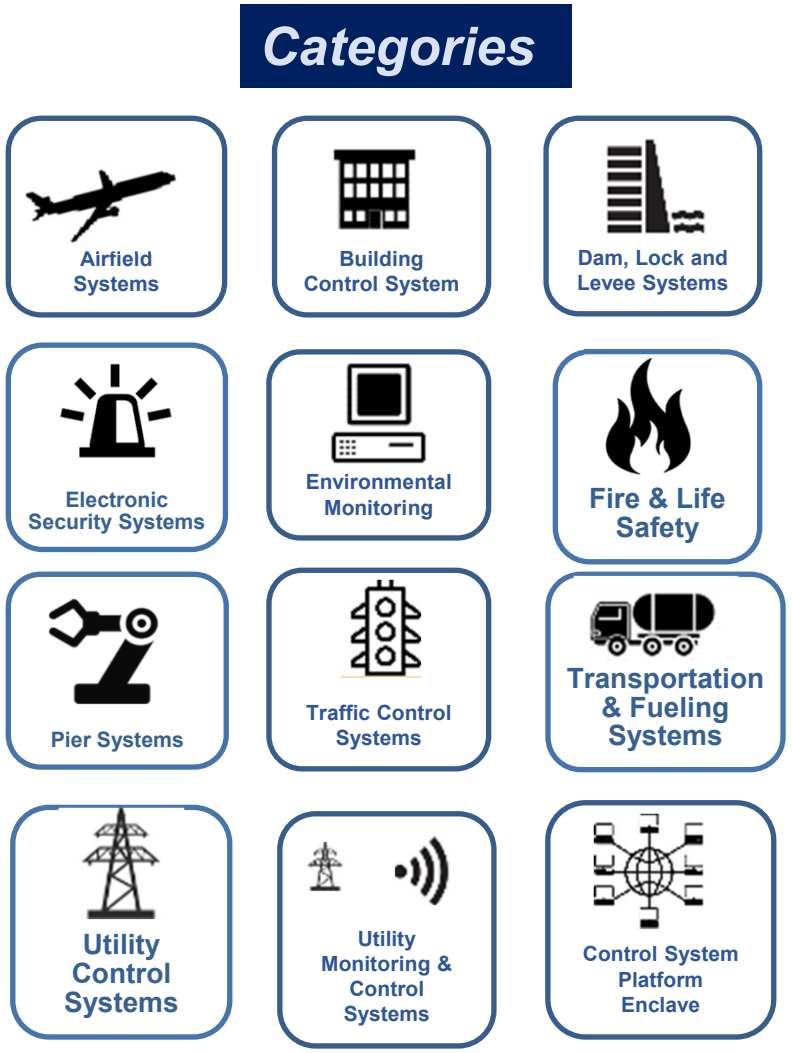
- **Demonstration Site**:
  - Fort Meade, MD
  - Langley AFB, Lackland AFB, Andrews AFB, Beale AFB
  - Fort Gordon

- **Performers**:
  - Billy Rios, Jonathan Butts | QED Secure

Operational Technology and FRCS

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

DoD Facility Related Control Systems (FRCS)

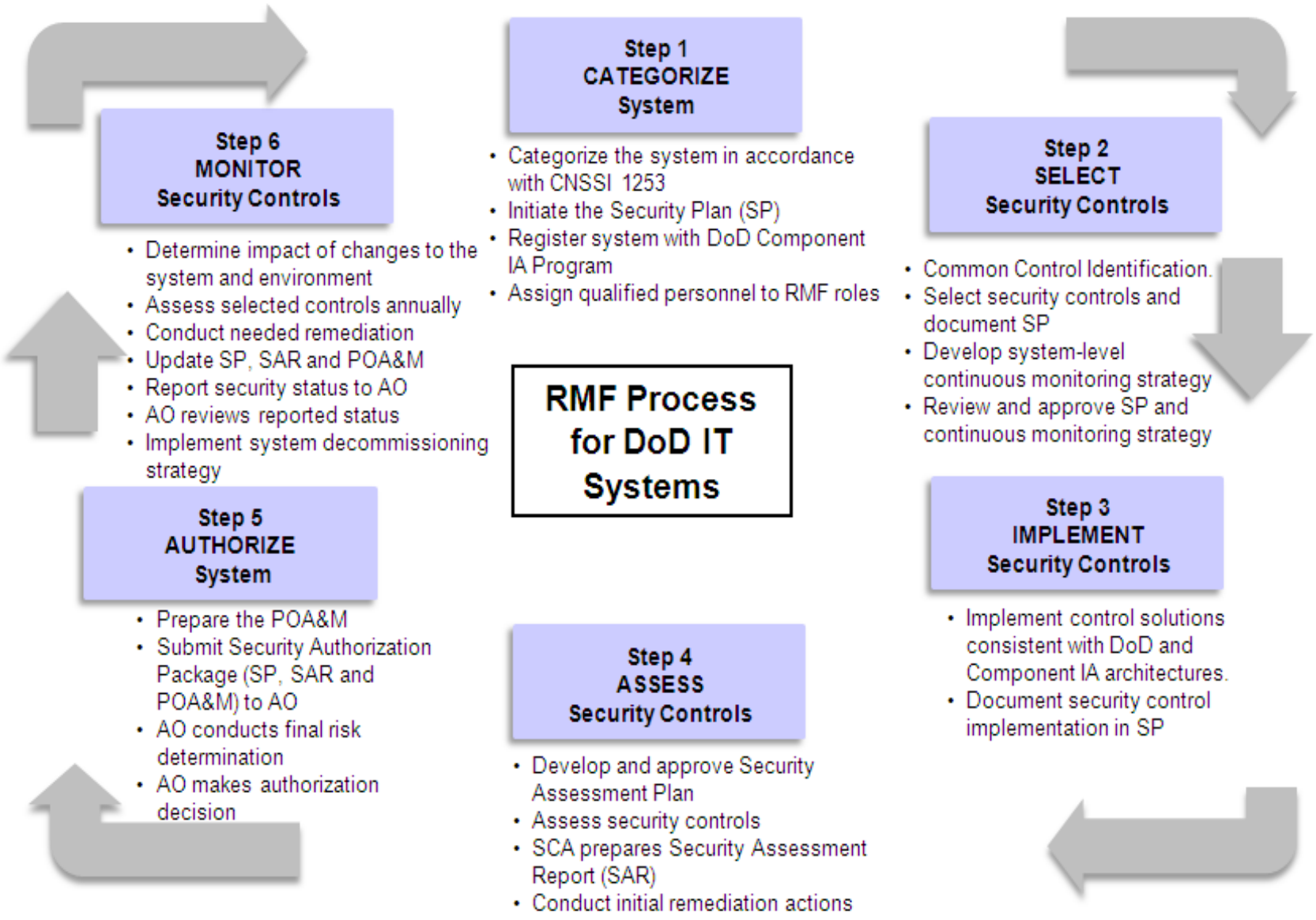


Systems

- 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?

FRCS Overlay & RMF Implementation



UFC Reference Architecture

Air Force

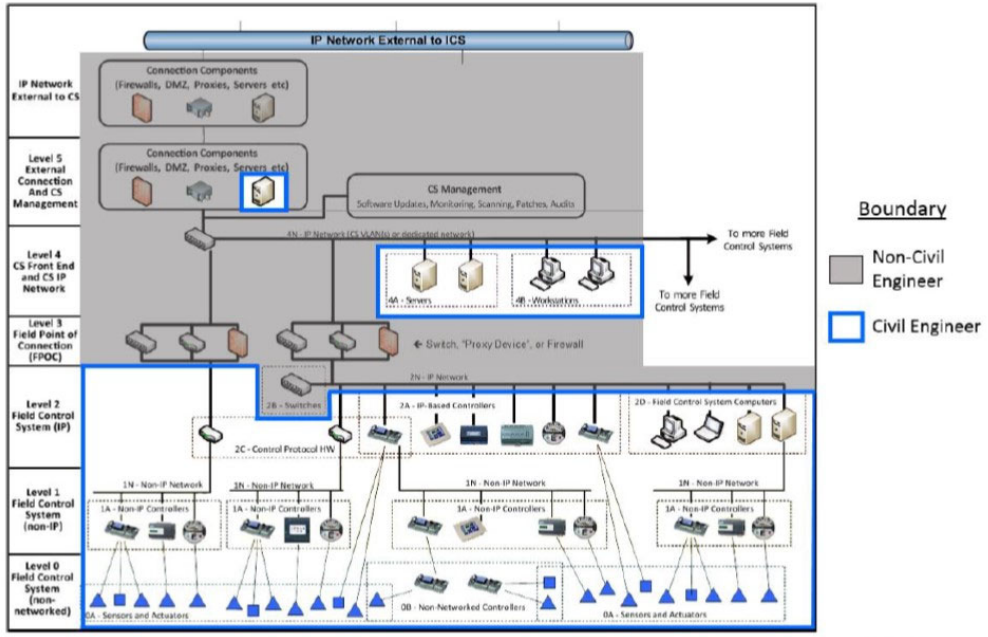
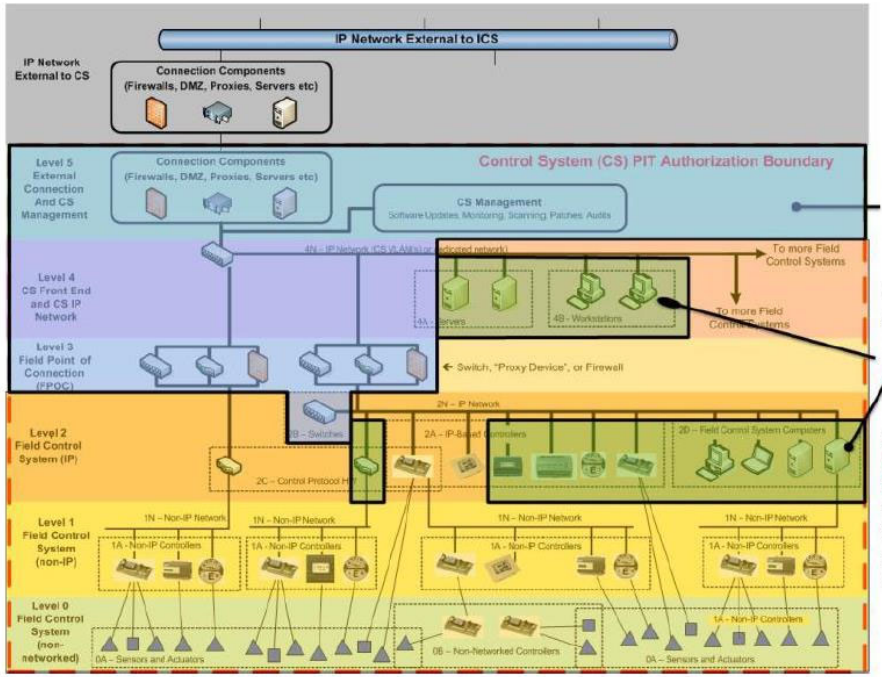


Figure 2-1: Topology of Control Systems and CE's Boundary of Responsibility

Navy



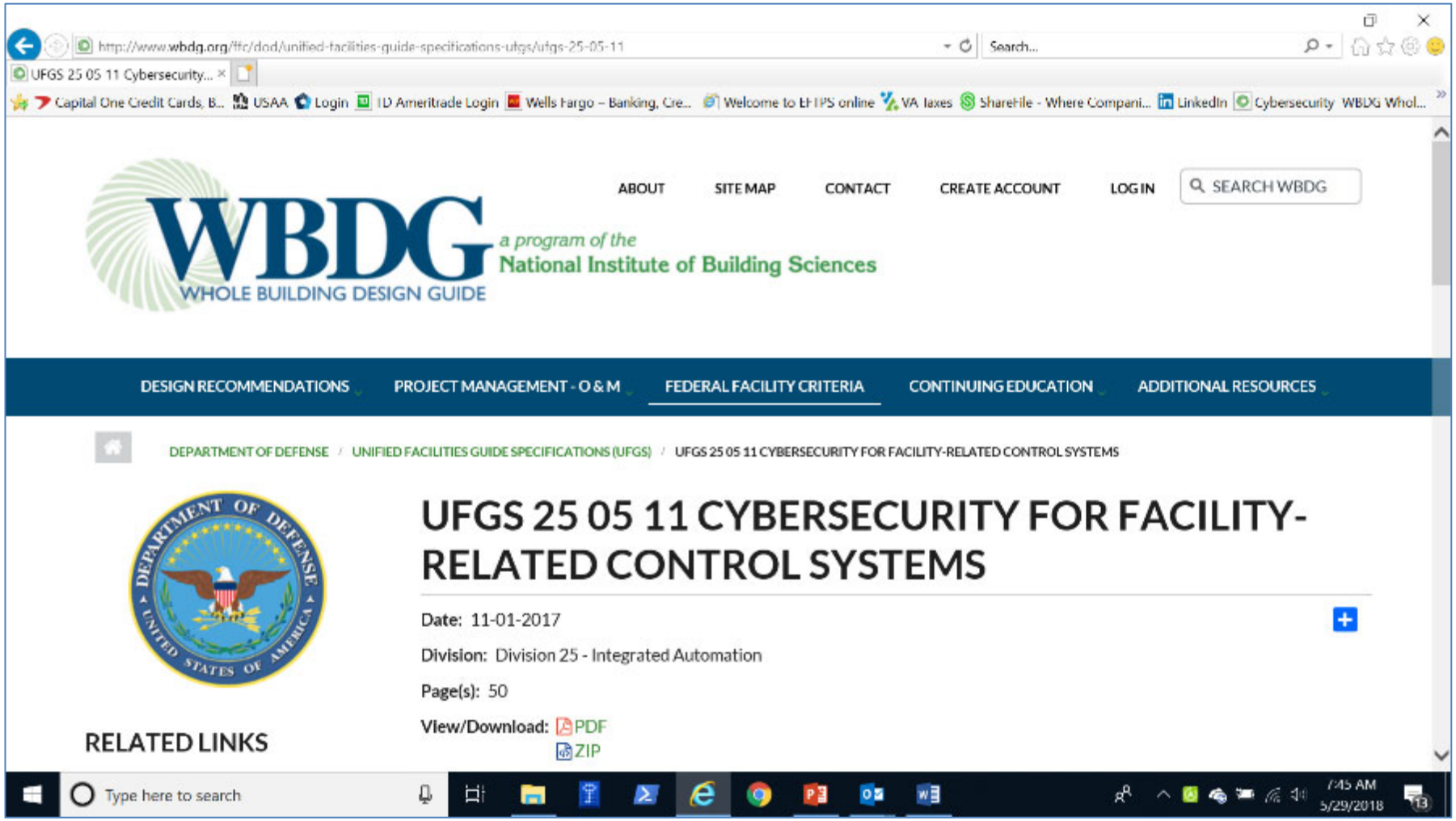
Platform Enclave (PE)

Operational Architecture (OA)

Navy Only: OA1: N-UMCS

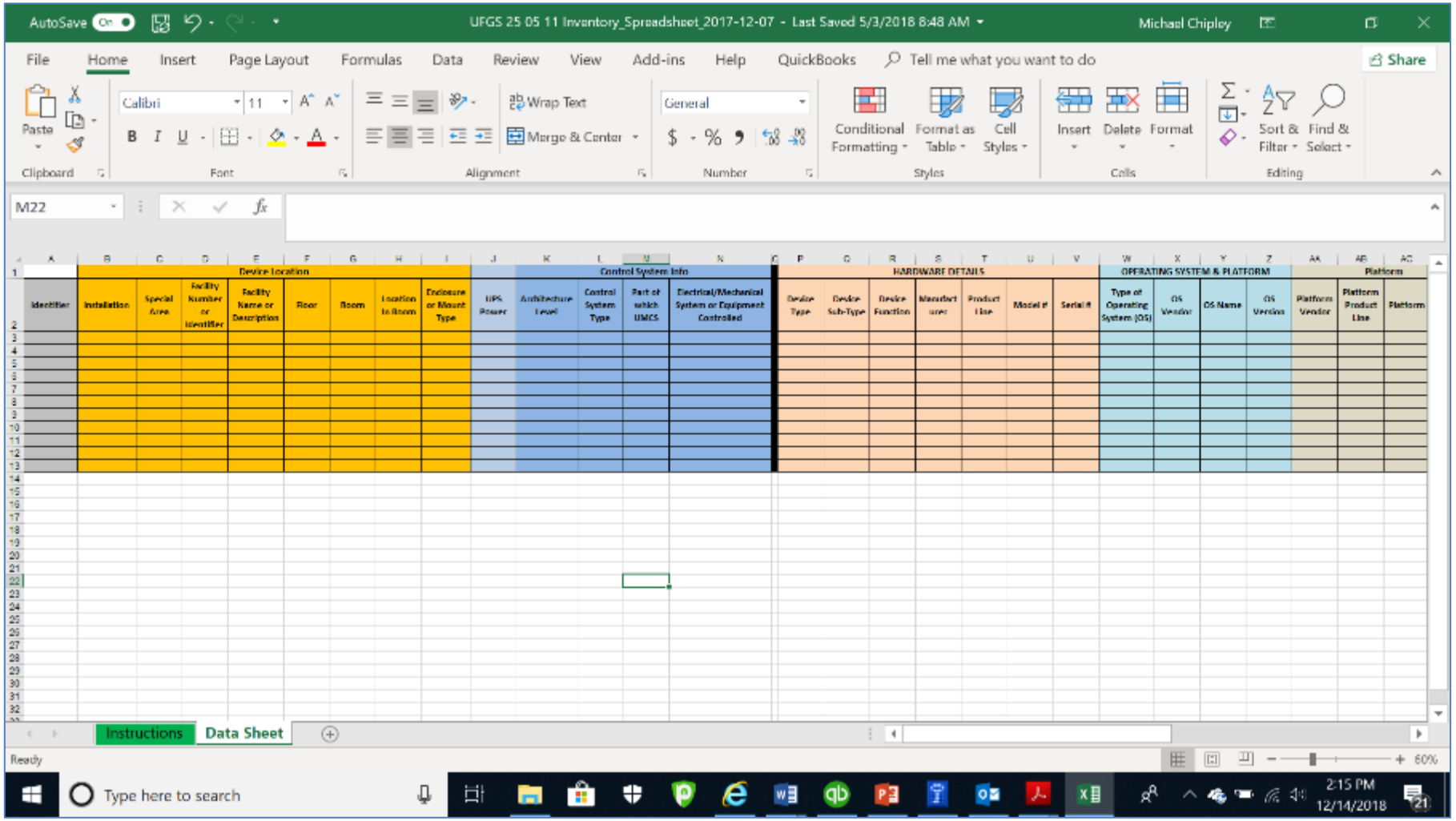
Navy Only: OA2
All else in Levels 0-2: FCS or UMCS requiring separate accreditation prior to connecting to N-UMCS and the PE

UFGS 25 05 11 Cybersecurity For FRCS



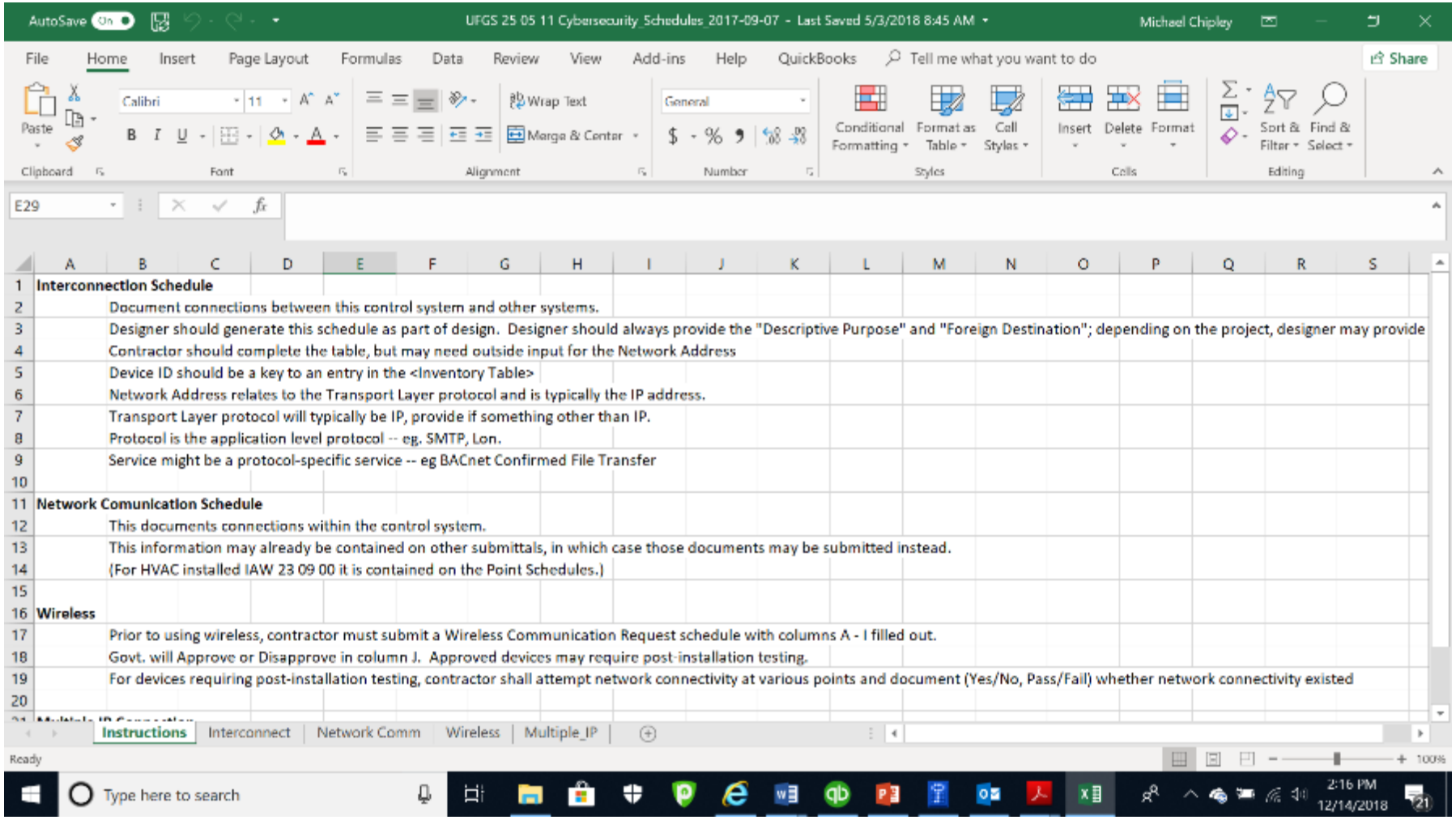
http://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-25-05-11

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



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

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

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

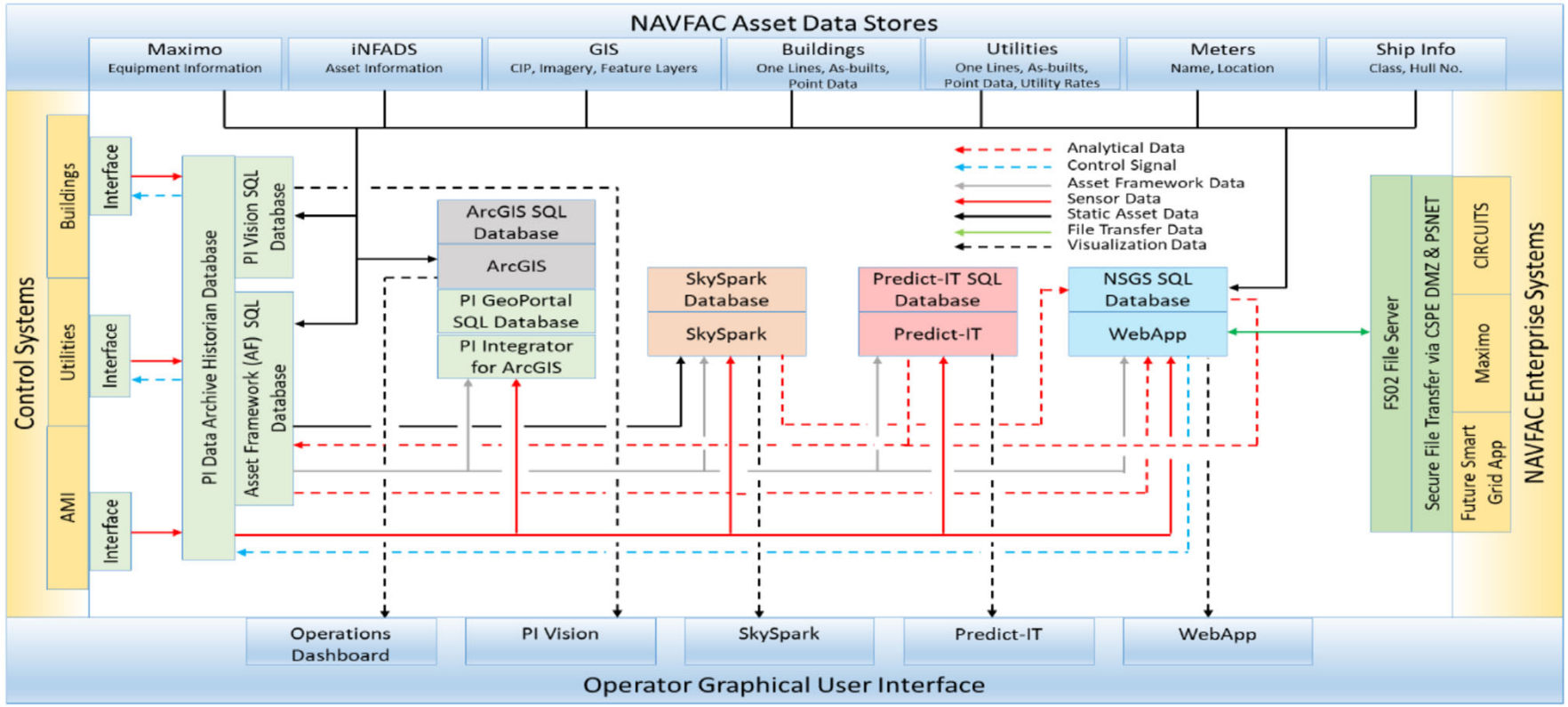
The Integrated Facility Management Systems (IFMS), and all control systems including related communications networks and components, are considered Platform Information Technology (PIT). Design and provide all control systems in accordance with UFC 4-010-06 "Cybersecurity of Facility-Related Control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

Navy Smart Grid

Smart Grid System Description



Tara Houlden

NAVFAC Cybersecurity Director

Kevin Whitt

KBR Smart Grid Project Manager

Energy Exchange 2019

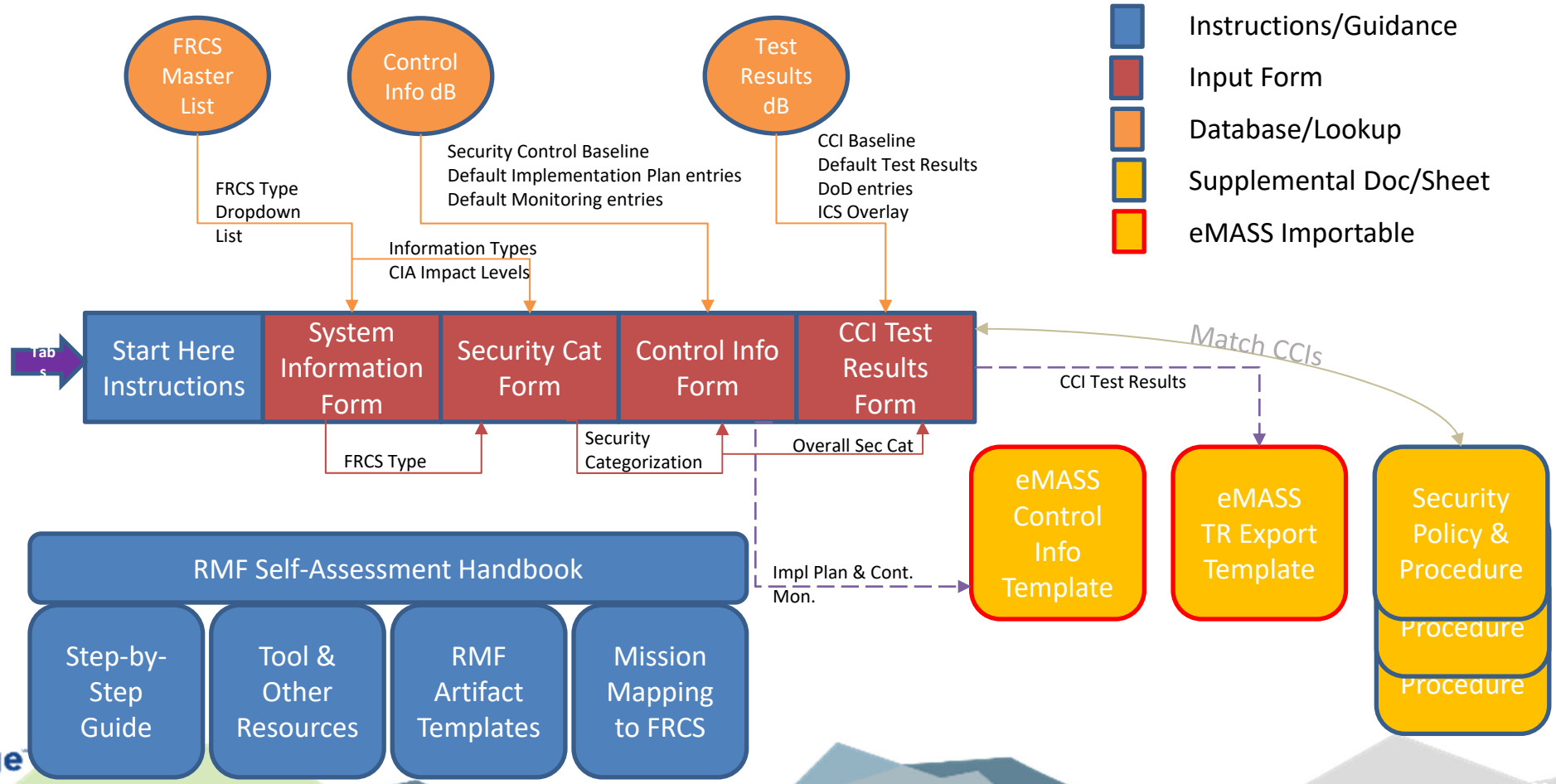
Navy Smart Grid Lessons Learned

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

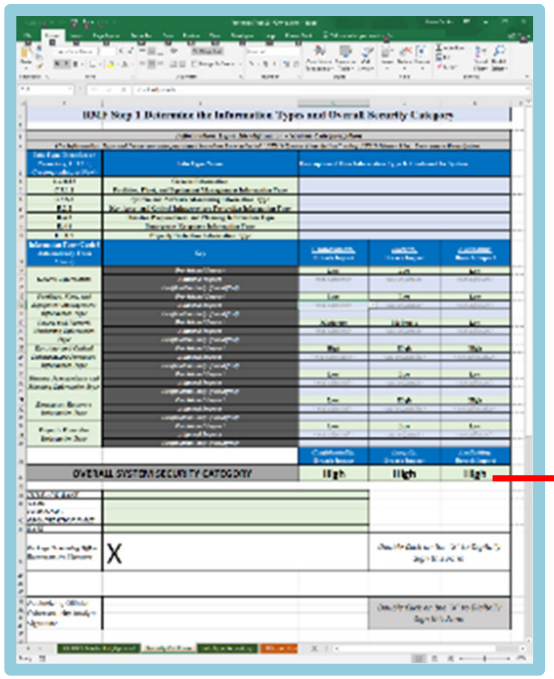
ESCTP FRCS RMF Tool



ESCTP FRCS RMF Tool

Step 3
Implement Controls

CCI Test Results Form

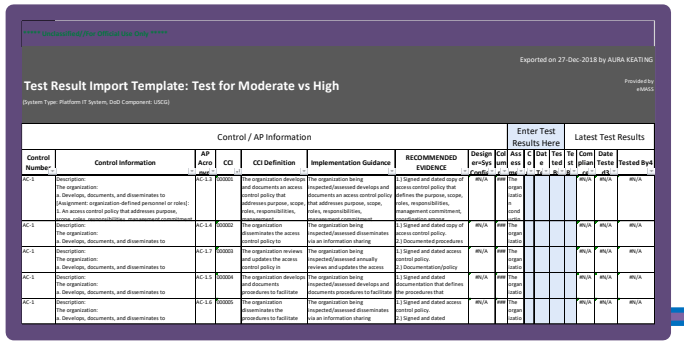


Security Categorization Form

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

30

Switching Gears….

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

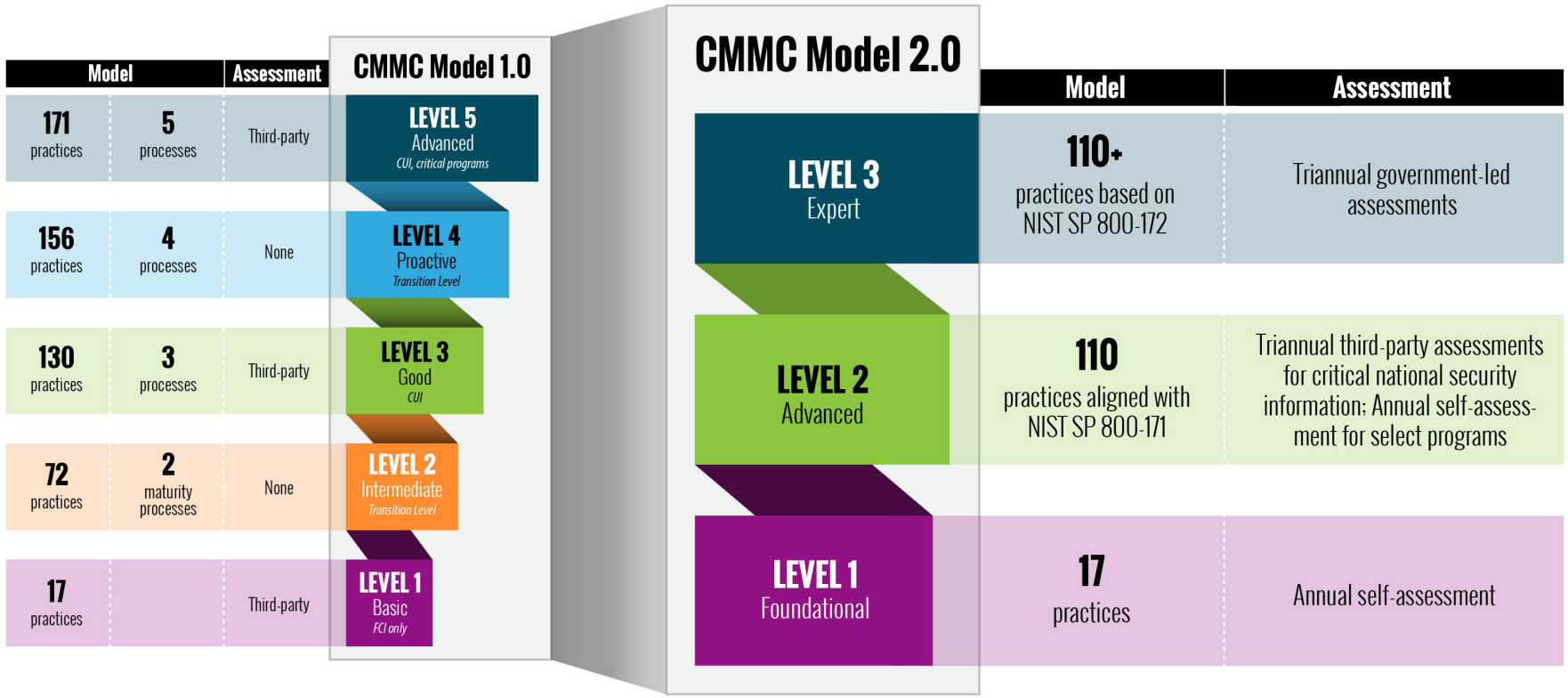
ESTCP FRCS Protecting CUI

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

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.**

CMMC 2.0 – Nov 2021



b) allow companies associated with the new Level 1 (Foundational) and some Level 2 (Advanced) acquisition programs to perform self-assessments rather than third-party assessments

Spirit of collaboration: Allows companies, under certain limited circumstances, to make Plans of Action & Milestones (POA&Ms) to achieve certification

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