Cybersecuring Control Systems, Cyber Training and Cybersecurity Compliance Maturity Model Updates

Michael Chipley PhD GICSP PMP LEED AP

INTRODUCTION

This article is a recap of a presentation given to the Federal Facilities Council in December 2022 that was a review of current activities underway at federal agencies, private sector, and industry associations to cybersecure control systems (HVAC, Fire and Mass Notification, Lighting, SCADA, etc.). The recent Executive Order and Legislation as well as on-going cyber campaigns to exploit control systems require the A&E, Construction, Operations and all staff involved with infrastructure services require new skills and certifications to properly design, construct and operate the CS. Specialized skills in Hunt and Defend, forensics and Incident Response are rapidly evolving. The session will provide an overview of the Society of American Military Engineers (SAME) Cybersecurity Inter Governmental Engagement effort, the International Society of Automation Incident Command System for Industrial Control System, the Building Cybersecurity organization and the DoD Cybersecurity Maturity Model Certification.

CYBERSECURING CONTROL SYSTEMS

In the past decade, cybersecuring control systems has become a new reality in the design, construction and operations of facilities and the related control systems (HVAC, Fire and Mass Notification, Lighting, SCADA, etc.). As an example of the shift, in 2009 the Department of Defense (DoD) initiated a program to develop Smart Installations to take advantage of the new technologies based on the use of traditional IT and the Internet to dramatically cut energy and water consumption costs. The concept was to integrate the control systems with business systems and enterprise systems to provide in real time the data and analytics to manage the ever more complex integrated systems and eliminate the need for manual operations.

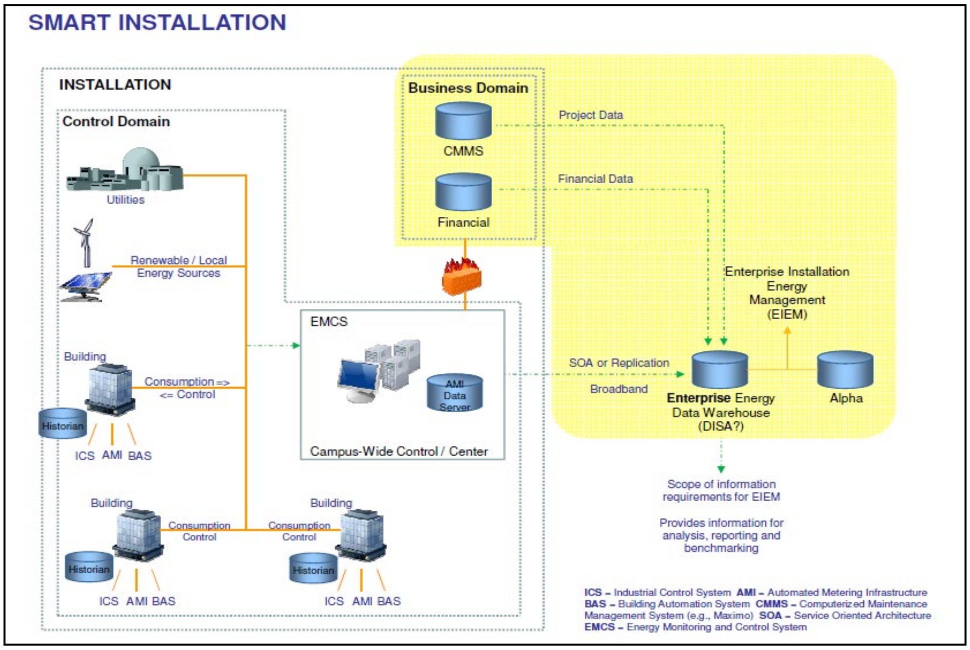
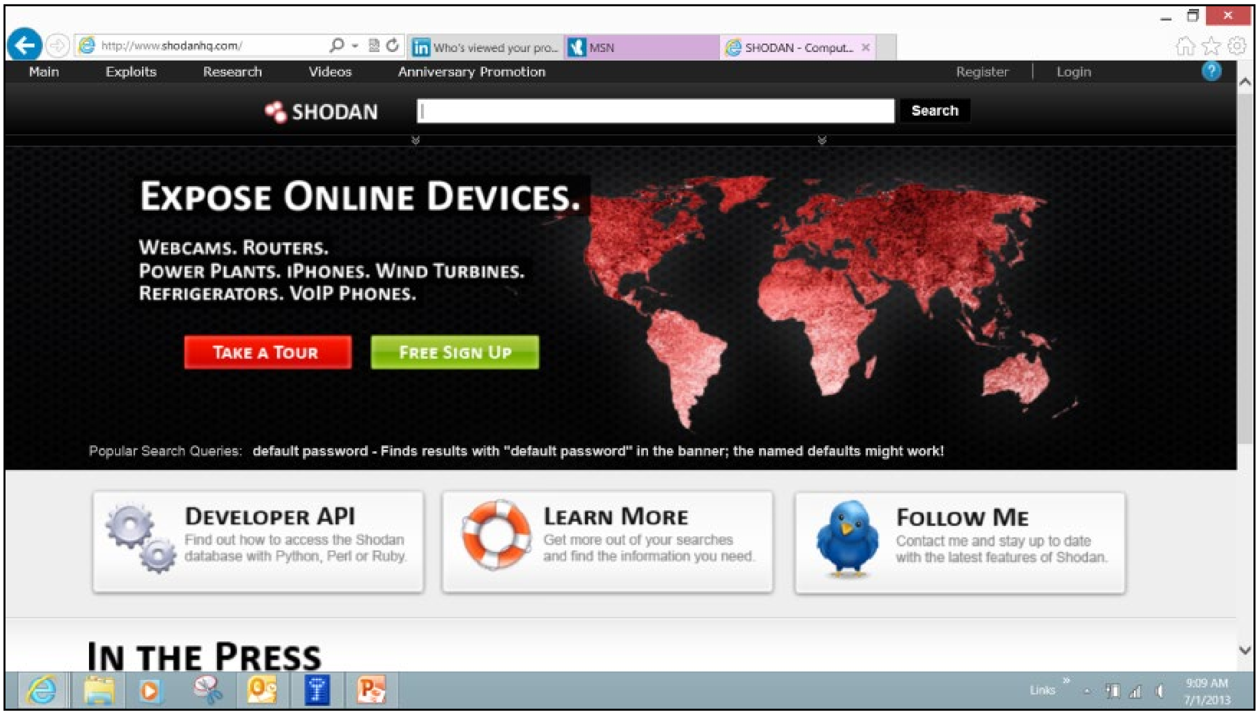

SMART INSTALLATION
INSTALLATION
Control Domain
Utilities
Renewable / Local Energy Sources
Building
Consumption => <= Control
Historian
ICS AMI BAS
Building
Consumption Control
Historian
ICS AMI BAS
Building
Consumption Control
Historian
ICS AMI BAS
EMCS
AMI Data Server
Campus-Wide Control / Center
Business Domain
CMMS
Financial
Project Data
Financial Data
Enterprise Installation Energy Management (EIEM)
SOA or Replication
Broadband
Enterprise Energy Data Warehouse (DISA?)
Alpha
Scope of information requirements for EIEM
Provides information for analysis, reporting and benchmarking
ICS – Industrial Control System AMI – Automated Metering Infrastructure
BAS – Building Automation System CMMS – Computerized Maintenance Management System (e.g., Maximo) SOA – Service Oriented Architecture
EMCS – Energy Monitoring and Control System

Figure 1 – DoD Smart Installation Concept

Around the same time, a new search tool called Shodan was released that did Internet searches for any IP connected device. Very quickly Shodan began to collect the metadata and catalogue IP devices such as cameras, controllers, HVAC systems, etc.



EXPOSE ONLINE DEVICES.

WEBCAMS. ROUTERS.
POWER PLANTS. IPHONES. WIND TURBINES.
REFRIGERATORS. VOIP PHONES.

Popular Search Queries: default password - Finds results with "default password" in the banner; the named defaults might work!

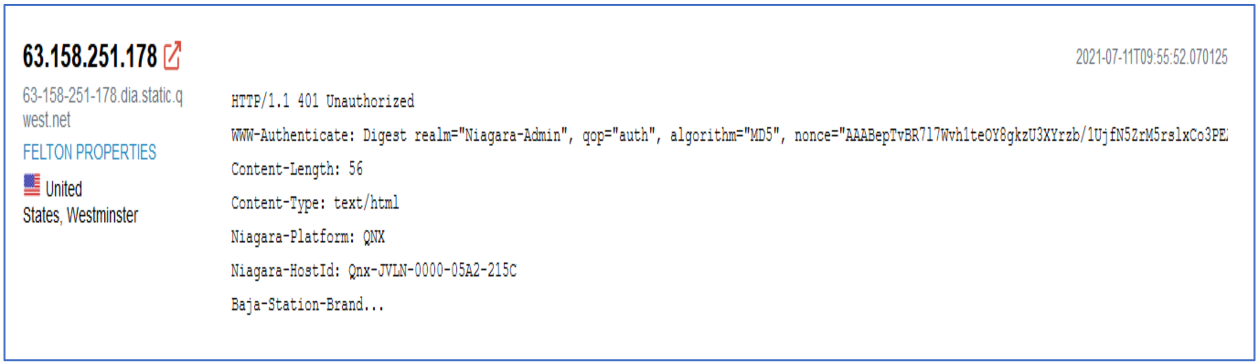
DEVELOPER API
Find out how to access the Shodan database with Python, Perl or Ruby.

LEARN MORE
Get more out of your searches and find the information you need.

FOLLOW ME
Contact me and stay up to date with the latest features of Shodan.

Figure 2– Shodan Homepage

Very quickly Shodan began to expose the control systems and misconfigurations that left the systems open to being exploited, and very few of the System Owners (SO) did not even realize their systems were exposed to the Internet and were in Shodan.



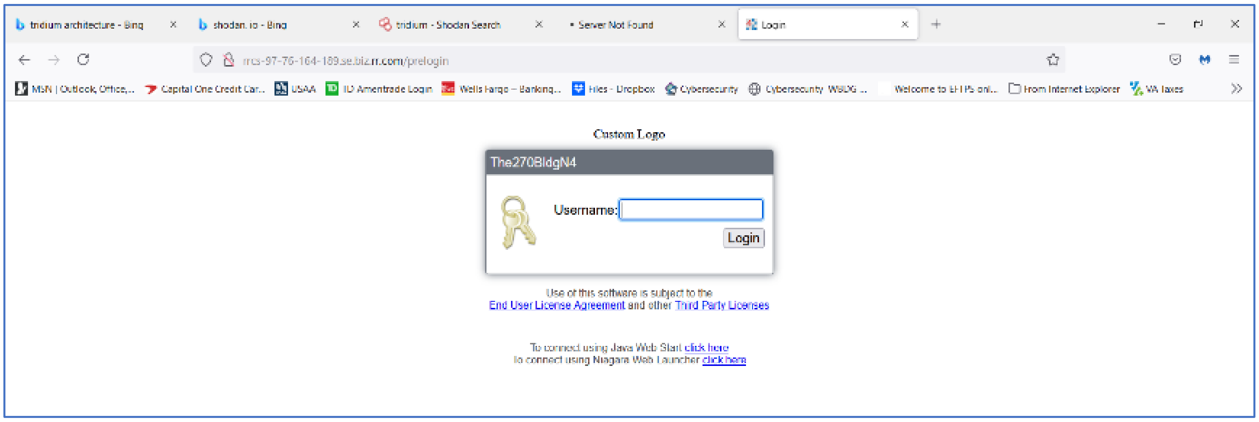
63.158.251.178
63-158-251-178.dia.static.qwest.net
FELTON PROPERTIES
United States, Westminster

2021-07-11T09:55:52.070125

```
HTTP/1.1 401 Unauthorized
WWW-Authenticate: Digest realm="Niagara-Admin", qop="auth", algorithm="MD5", nonce="AAABepTvBR717Wvh1teOY8gkzU3XYrzb/1UjfN5ZrM5rslxCo3PE
Content-Length: 56
Content-Type: text/html
Niagara-Platform: QNX
Niagara-HostId: Qnx-JVLN-0000-05A2-215C
Baja-Station-Brand...
```

Figure 3– Shodan Metadata of a Misconfigured Niagara HVAC system

Many of the control systems did not even require a login, or might have only had Username access, which in many cases was the Default password set up by the OEM vendor.



Custom Logo

The270BldgN4

Username:

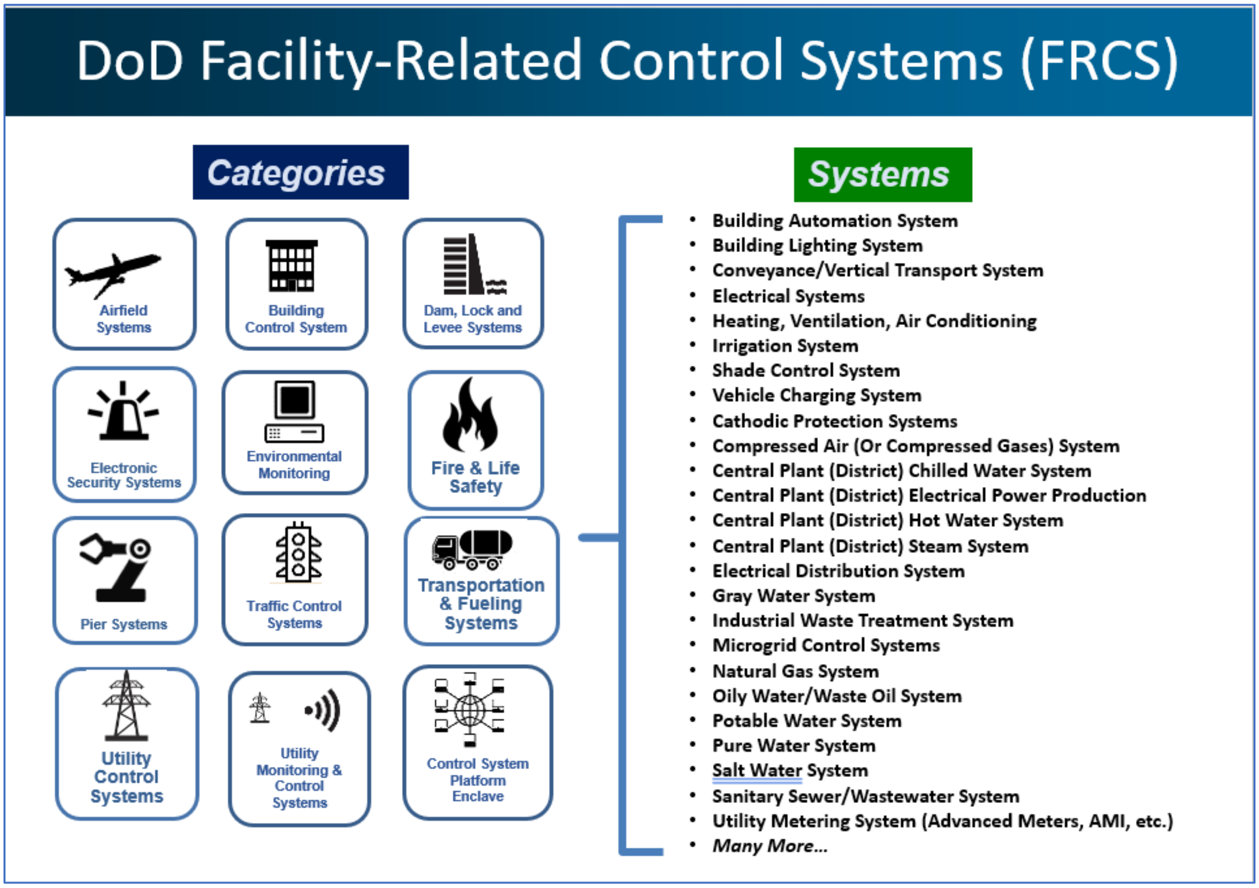
Login

Use of this software is subject to the
End User License Agreement and other Third Party Licenses

To connect using Java Web Start click here
To connect using Niagara Web Launcher click here

Figure 4– Shodan Username Login of a Misconfigured Niagara HVAC system

The DoD had a number of military installations that could be found in Shodan and it took a couple of years to determine how they appeared and how to have them removed. The DoD Facilities community then embarked on a journey to cybersecure the Facility-Related Control Systems (FRCS) by forming a Working Group and developing a Master List with Categories and Systems.



DoD Facility-Related Control Systems (FRCS)

Categories

- Airfield Systems
- Building Control System
- Dam, Lock and Levee Systems
- Electronic Security Systems
- Environmental Monitoring
- Fire & Life Safety
- Pier Systems
- Traffic Control Systems
- Transportation & Fueling Systems
- Utility Control Systems
- Utility Monitoring & Control Systems
- Control System Platform Enclave

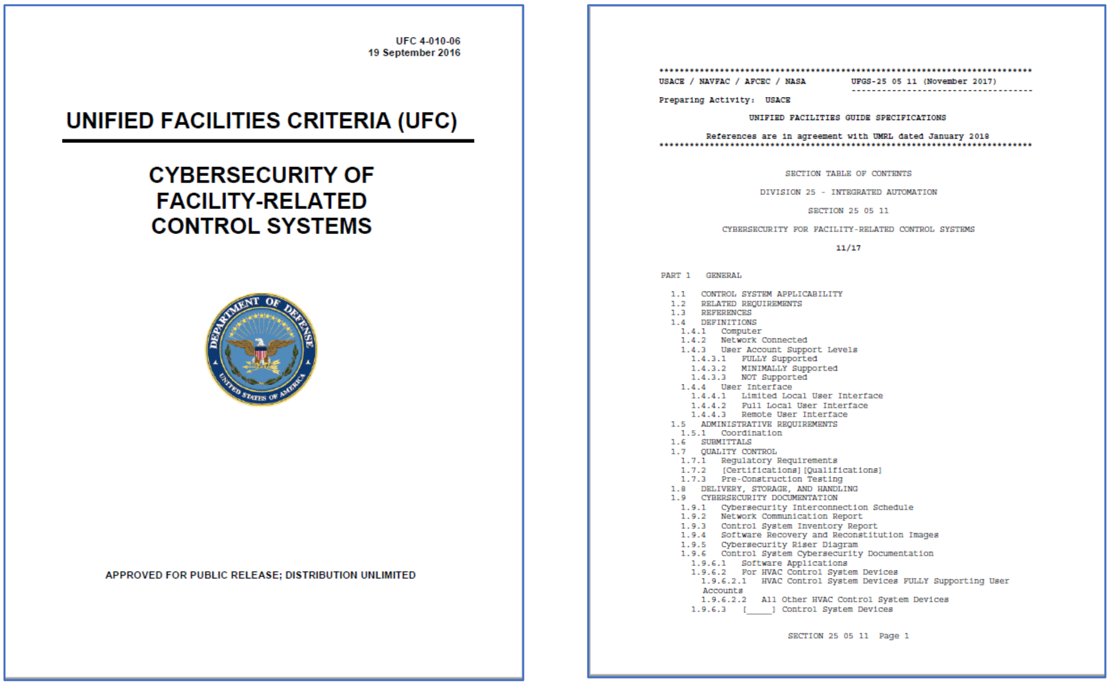
Systems

- **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…***

Figure 5 – DoD Facility-Related Control Systems Master List

The next step was to develop a Unified Facility Criteria (UFC) for the Architect-Engineering (A&E) community to design cybersecurity into a project that was released in 2016 followed by a Unified Facility

Guide Specification (UFGS) in 2017. The UFC established the Reference Architecture that would correlate with an Inventory and allow DoD to begin tracking all of the FRCS down to the IP controllers level.



UFC 4-010-06
19 September 2016

UNIFIED FACILITIES CRITERIA (UFC)

CYBERSECURITY OF
FACILITY-RELATED
CONTROL SYSTEMS

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

USACE / NAVFAC / AFCEC / NASA UFGS-25 05 11 (November 2017)

Preparing Activity: USACE

UNIFIED FACILITIES GUIDE SPECIFICATIONS

References are in agreement with UMRL dated January 2018

SECTION TABLE OF CONTENTS

DIVISION 25 - INTEGRATED AUTOMATION

SECTION 25 05 11

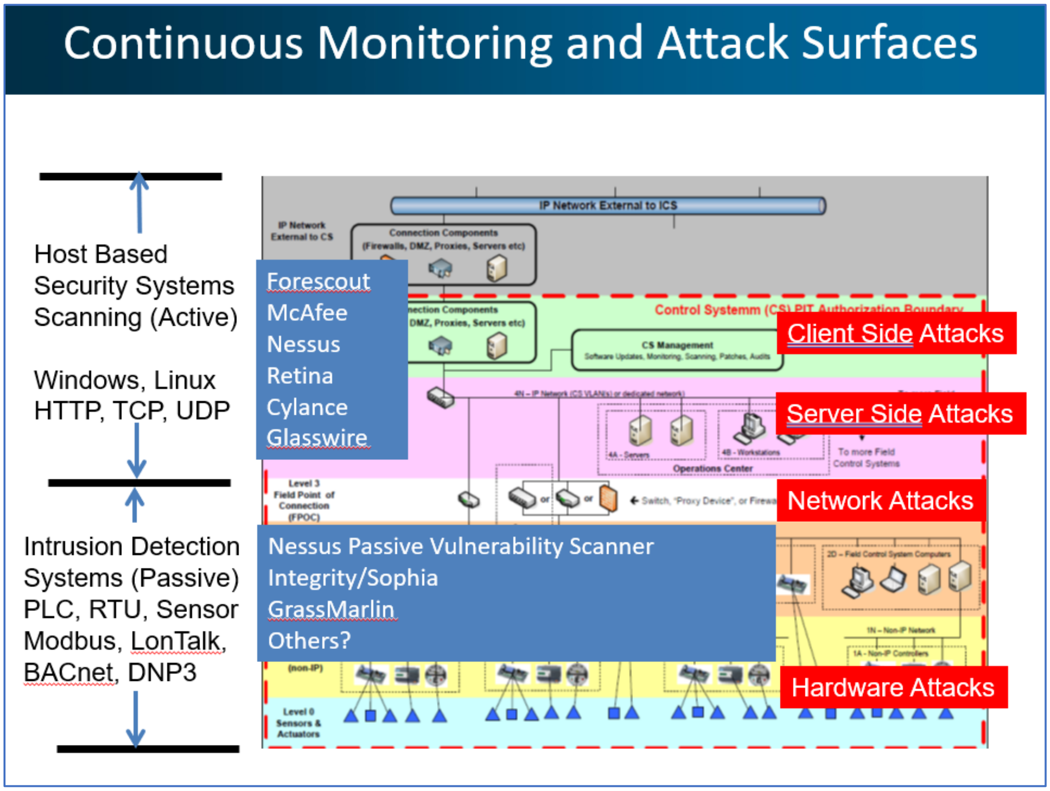
CYBERSECURITY FOR FACILITY-RELATED CONTROL SYSTEMS

11/17

PART 1 GENERAL

SECTION 25 05 11 Page 1

Figure 6 - DoD Facility-Related Control Systems UFC and UFGS



Continuous Monitoring and Attack Surfaces

Host Based
Security Systems
Scanning (Active)

Windows, Linux
HTTP, TCP, UDP

Intrusion Detection
Systems (Passive)
PLC, RTU, Sensor
Modbus, LonTalk,
BACnet, DNP3

Forescout
McAfee
Nessus
Retina
Cylance
Glasswire

Nessus Passive Vulnerability Scanner
Integrity/Sophia
GrassMarlin
Others?

Client Side Attacks

Server Side Attacks

Network Attacks

Hardware Attacks

IP Network External to ICS
IP Network External to CS
Connection Components (Firewalls, DMZ, Proxies, Servers etc)
Control Systemm (CS) PIT Authorization Boundary
CS Management
Software Updates, Monitoring, Scanning, Patches, Audits
4N – IP Network (CS VLAN(s) or dedicated network)
4A - Servers
4B - Workstations
Operations Center
To more Field Control Systems
Level 3 Field Point of Connection (FPOC)
or
Switch, "Proxy Device", or Firewa
2D – Field Control System Computers
1N – Non-IP Network
1A – Non-IP Controllers
(non-IP)
Level 0 Sensors & Actuators

Figure 7 – DoD UFC Facility-Related Control Systems Reference Architecture

The new UFC and UFGS were added to the contracting language for DoD Design and Construction contracts in 2017 and the first round of contractors complying with the new requirements was underway. Working with the OEM vendors, the control systems equipment and front ends underwent upgrades and enhanced security features; new technologies such as Virtual Machines and Cloud services provided additional cybersecurity capabilities and enabled the creation of the Smart Building.

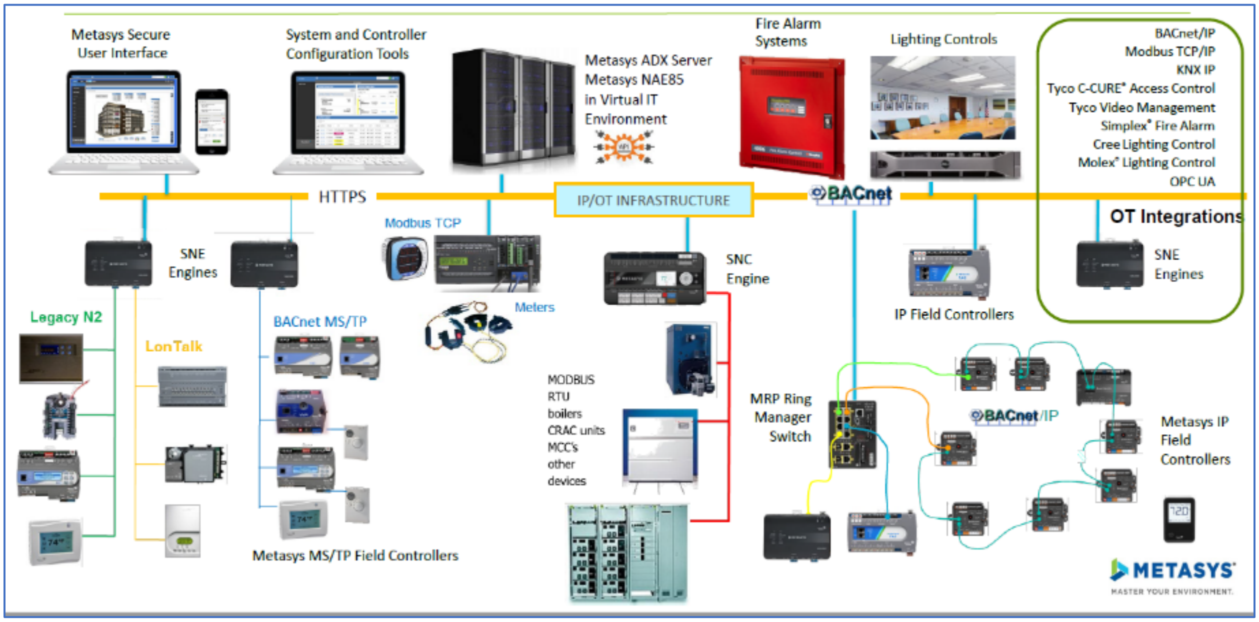


Figure 8 – Johnson Control Systems Metasys Building Management System

The next evolution now underway is the Grid-Interactive Efficient Building (GEB) which uses the Smart Building technologies to interact with the national electric grid and become net zero consumption and net zero carbon emissions (or as close as practical as possible).

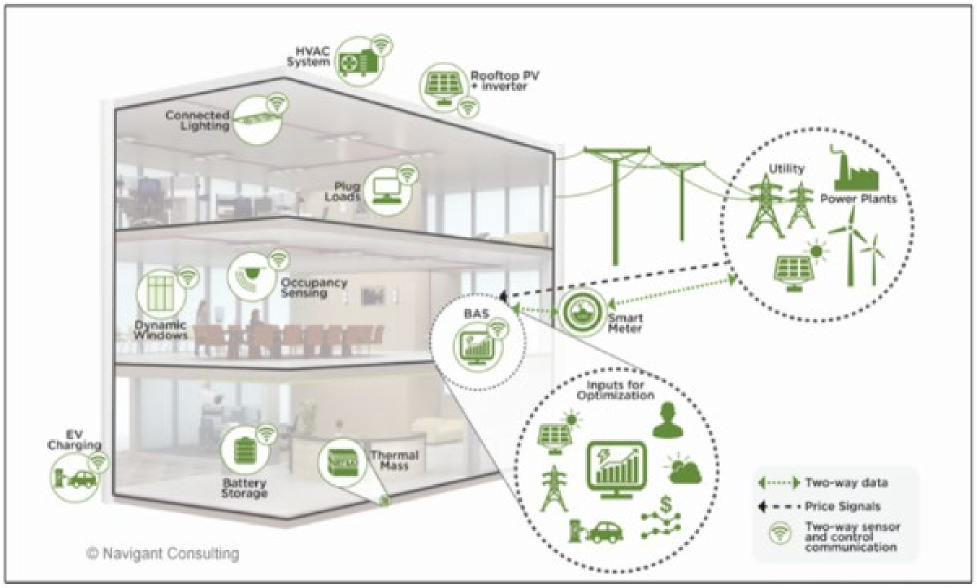


Figure 9 – Grid-Interactive Efficient Buildings

CYBERSECURITY TRAINING EFFORTS IN INDUSTRY AND ORGANIZATIONS

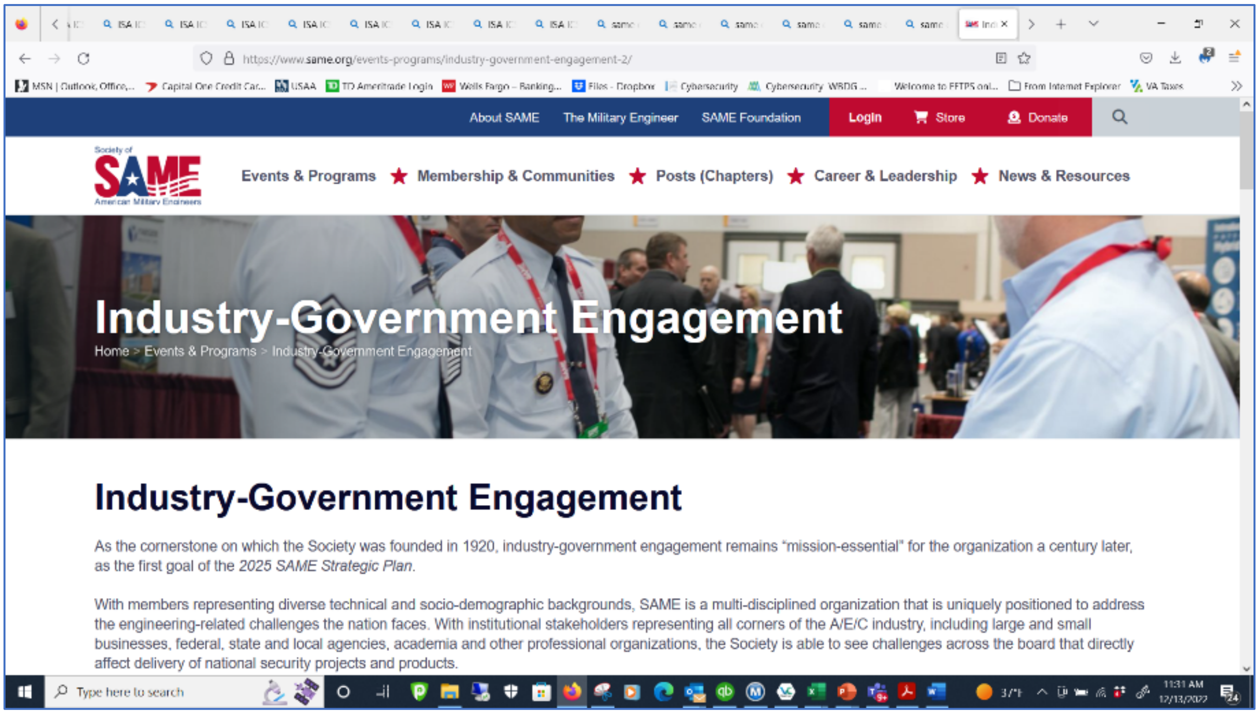
The need to educate and train the Facilities community on cybersecuring these control systems has become a major effort across several organizations. The Society of American Military Engineers (SAME) launched the Cyber Industry-Governmental Engagement (IGE) effort in 2022.

Mission

- Increase understanding and mitigate cybersecurity risks to physical infrastructure and facilities owned and/or operated by federal agencies
- Identify ways that SAME can support federal agency partners in mitigating those risks.

Key Focus Areas :

- Identify/evaluate OT related risks to federal missions, assets, and personnel
- Cultivate cyber risk subject matter expertise both in industry and federal agencies
- Engage leading experts in protection of OT in building management systems
- Engage the facility engineering team in federal agencies
- Develop content in support of federal policy development



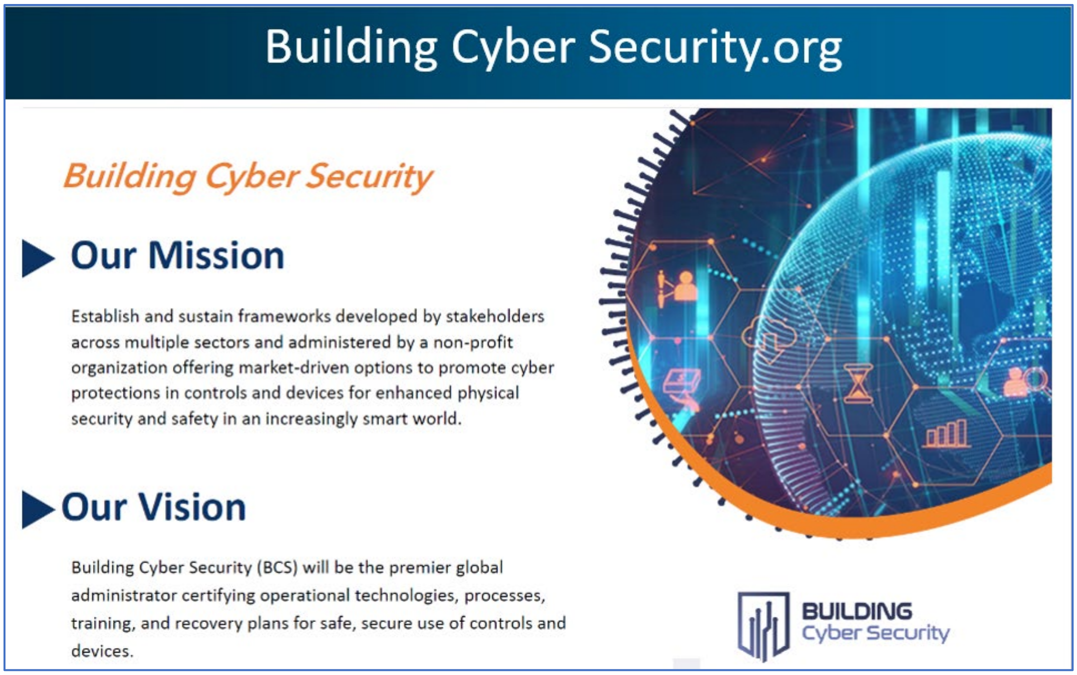
Industry-Government Engagement

As the cornerstone on which the Society was founded in 1920, industry-government engagement remains "mission-essential" for the organization a century later, as the first goal of the *2025 SAME Strategic Plan*.

With members representing diverse technical and socio-demographic backgrounds, SAME is a multi-disciplined organization that is uniquely positioned to address the engineering-related challenges the nation faces. With institutional stakeholders representing all corners of the A/E/C industry, including large and small businesses, federal, state and local agencies, academia and other professional organizations, the Society is able to see challenges across the board that directly affect delivery of national security projects and products.

Figure 10 – SAME Cyber IGE Program

The SAME IGE is a partner with the Building Cyber Security Organization to further develop the resources and training across the communities. The BCS has developed a Risk Score and rating system that building owners, insurers and tenants can use as a metric for Facility Cyber Security Risk.



Building Cyber Security.org

Building Cyber Security

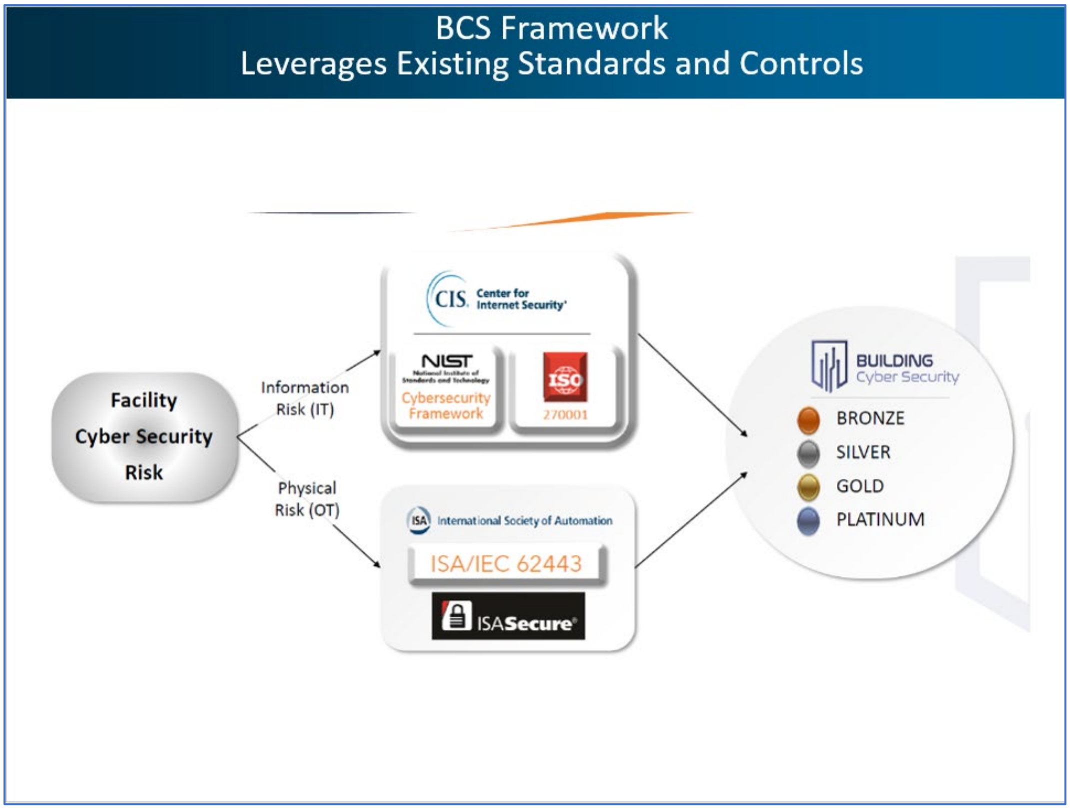
▶ Our Mission

Establish and sustain frameworks developed by stakeholders across multiple sectors and administered by a non-profit organization offering market-driven options to promote cyber protections in controls and devices for enhanced physical security and safety in an increasingly smart world.

▶ Our Vision

Building Cyber Security (BCS) will be the premier global administrator certifying operational technologies, processes, training, and recovery plans for safe, secure use of controls and devices.

Figure 11 – Building Cyber Security Organization

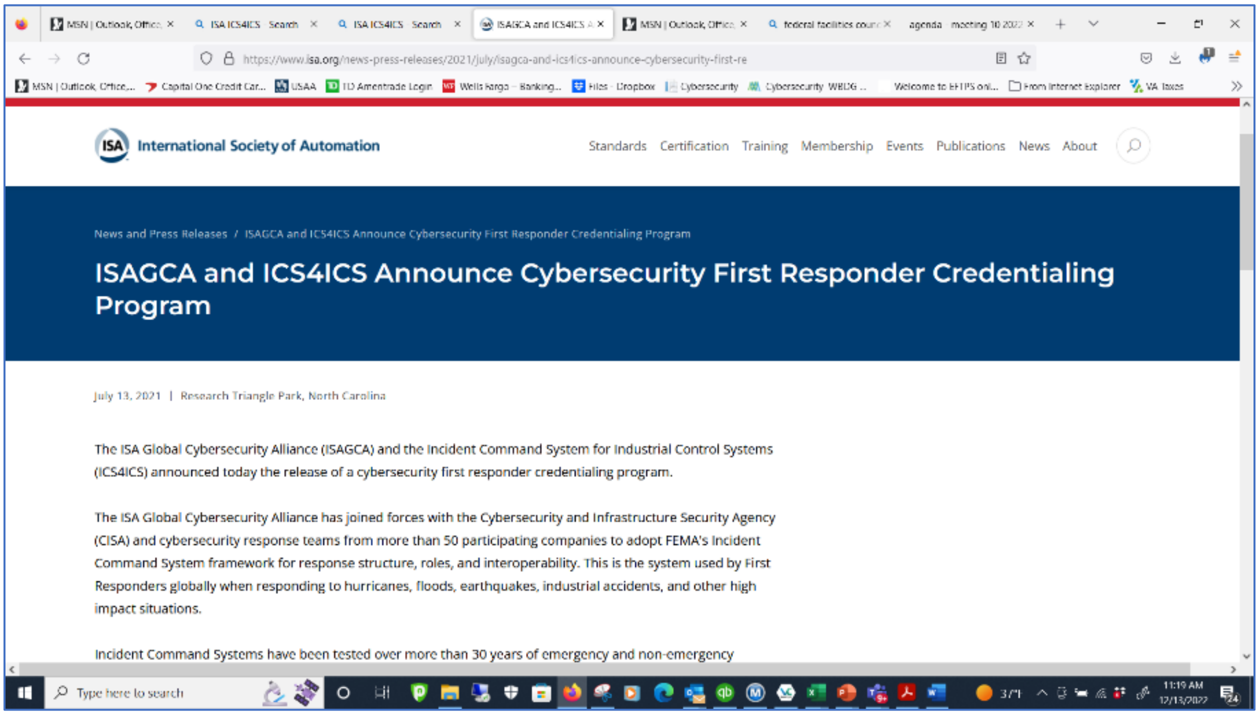


BCS Framework
Leverages Existing Standards and Controls

Figure 12 – BCS Framework for Facility Cyber Security Risk

Note the connection to the International Society of Automation ISA 62443 standard. The ISA is the lead organization to develop the Incident Command System for Industrial Control Systems (ICS4ICS) First Responders Credentialing Program.

> “Incident Command System for Industrial Control Systems (ICS4ICS) is designed to improve global Industrial Control System cybersecurity incident management capabilities. ICS4ICS will leverage the Incident Command System, as outlined by FEMA, for response structure, roles, and interoperability. The Incident Command System is used by First Responders globally every day when responding to motor vehicle accidents, small and large fires, hurricanes, floods, earthquakes, industrial accidents, and other high impact situations. The Incident Command System has been tested for more than 30 years of emergency and non-emergency applications, throughout all levels of government and within the private sector.
>
> The ISA Global Cybersecurity Alliance has joined forces with the Cybersecurity and Infrastructure Security Agency (CISA) and cybersecurity response teams from more than 50 participating companies to adopt the Incident Command System, as outlined by FEMA, for response structure, roles, and interoperability. This is the system used by First Responders worldwide daily when responding to very small and very large emergency situations like motor vehicle accidents, fires, to hurricanes, floods, earthquakes, industrial accidents, and other high impact situations.”



News and Press Releases / ISAGCA and ICS4ICS Announce Cybersecurity First Responder Credentialing Program

ISAGCA and ICS4ICS Announce Cybersecurity First Responder Credentialing Program

July 13, 2021 | Research Triangle Park, North Carolina

The ISA Global Cybersecurity Alliance (ISAGCA) and the Incident Command System for Industrial Control Systems (ICS4ICS) announced today the release of a cybersecurity first responder credentialing program.

The ISA Global Cybersecurity Alliance has joined forces with the Cybersecurity and Infrastructure Security Agency (CISA) and cybersecurity response teams from more than 50 participating companies to adopt FEMA's Incident Command System framework for response structure, roles, and interoperability. This is the system used by First Responders globally when responding to hurricanes, floods, earthquakes, industrial accidents, and other high impact situations.

Incident Command Systems have been tested over more than 30 years of emergency and non-emergency

Figure 13 – ICS4ICS Cybersecurity First Responder Credentialing Program

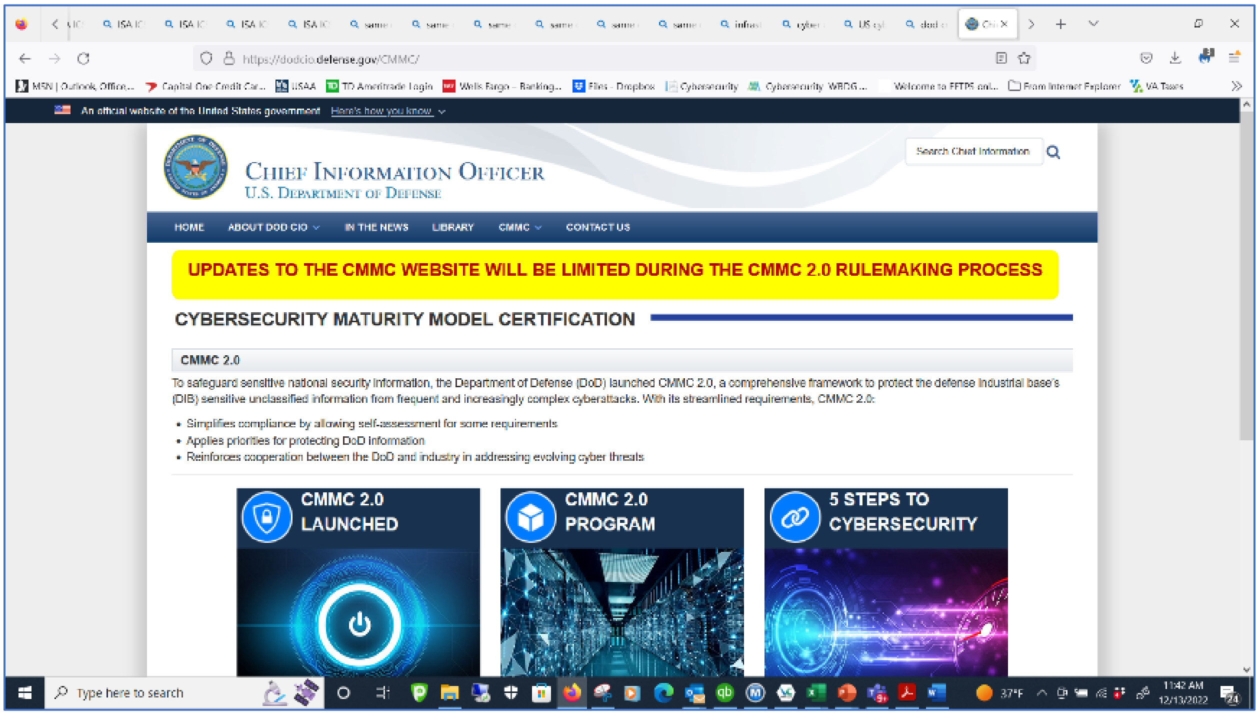
Lastly, the DoD is the first federal agency to require contractors and vendors to have a Cyber Risk Management Plan in place to secure their business systems that collect, store and transmit Controlled Unclassified Information (CUI).

DFARS 701 CLAUSE AND CREATING A NIST 800-171 COMPLIANT CYBER RISK MANAGEMENT PLAN (CRMP)

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. DoD issued the DFARS 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting in 2015 with compliance required by January 2018. **The intent is for an organization to be able to Detect a cyber incident and report it within 72 hours so that the compromise or breach can be evaluated for other impacts to DoD and/or contractor/vendor/Defense Industrial Base partners.**

(a) *Definitions*. As used in this clause—

> "Adequate security" means protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information.
>
> "Compromise" means disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred.
>
> "Contractor attributional/proprietary information" means information that identifies the contractor(s), whether directly or indirectly, by the grouping of information that can be traced back to the contractor(s) (e.g., program description, facility locations), personally identifiable information, as well as trade secrets, commercial or financial information, or other commercially sensitive information that is not customarily shared outside of the company.
>
> "Controlled technical information" means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions.
>
> "Covered contractor information system" means an unclassified information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information.



CHIEF INFORMATION OFFICER
U.S. DEPARTMENT OF DEFENSE

UPDATES TO THE CMMC WEBSITE WILL BE LIMITED DURING THE CMMC 2.0 RULEMAKING PROCESS

CYBERSECURITY MATURITY MODEL CERTIFICATION

CMMC 2.0

To safeguard sensitive national security information, the Department of Defense (DoD) launched CMMC 2.0, a comprehensive framework to protect the defense industrial base's (DIB) sensitive unclassified information from frequent and increasingly complex cyberattacks. With its streamlined requirements, CMMC 2.0:

- Simplifies compliance by allowing self-assessment for some requirements
- Applies priorities for protecting DoD information
- Reinforces cooperation between the DoD and industry in addressing evolving cyber threats

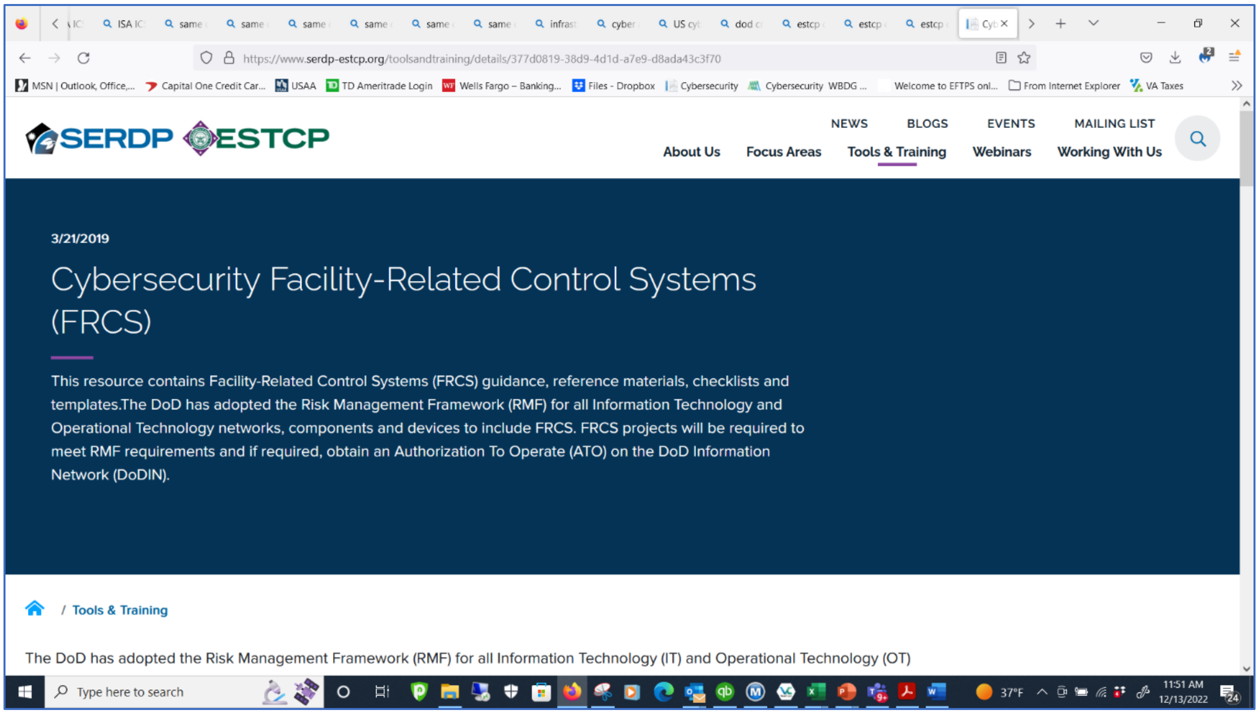
Figure 14 – Office of Secretary of Defense CIO CMMC Homepage

The DFARS 7012 Clause uses the **NIST SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations** standard as the basis of a cybersecurity program.

> “ 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. “

DoD ESTCP WEBSITE CYBER RISK MANAGEMENT PLAN TEMPLATES

The current 800-171 DFARS 7012 CRMP process is posted on the DoD ESCTP website at: https://serdp-estcp.org/Tools-and-Training/Installation-Energy-and-Water/Cybersecurity/FRCS-Protecting-CUI.



3/21/2019

Cybersecurity Facility-Related Control Systems (FRCS)

This resource contains Facility-Related Control Systems (FRCS) guidance, reference materials, checklists and templates.The DoD has adopted the Risk Management Framework (RMF) for all Information Technology and Operational Technology networks, components and devices to include FRCS. FRCS projects will be required to meet RMF requirements and if required, obtain an Authorization To Operate (ATO) on the DoD Information Network (DoDIN).

/ Tools & Training

The DoD has adopted the Risk Management Framework (RMF) for all Information Technology (IT) and Operational Technology (OT)

Figure 9 - DoD ESTPC Website

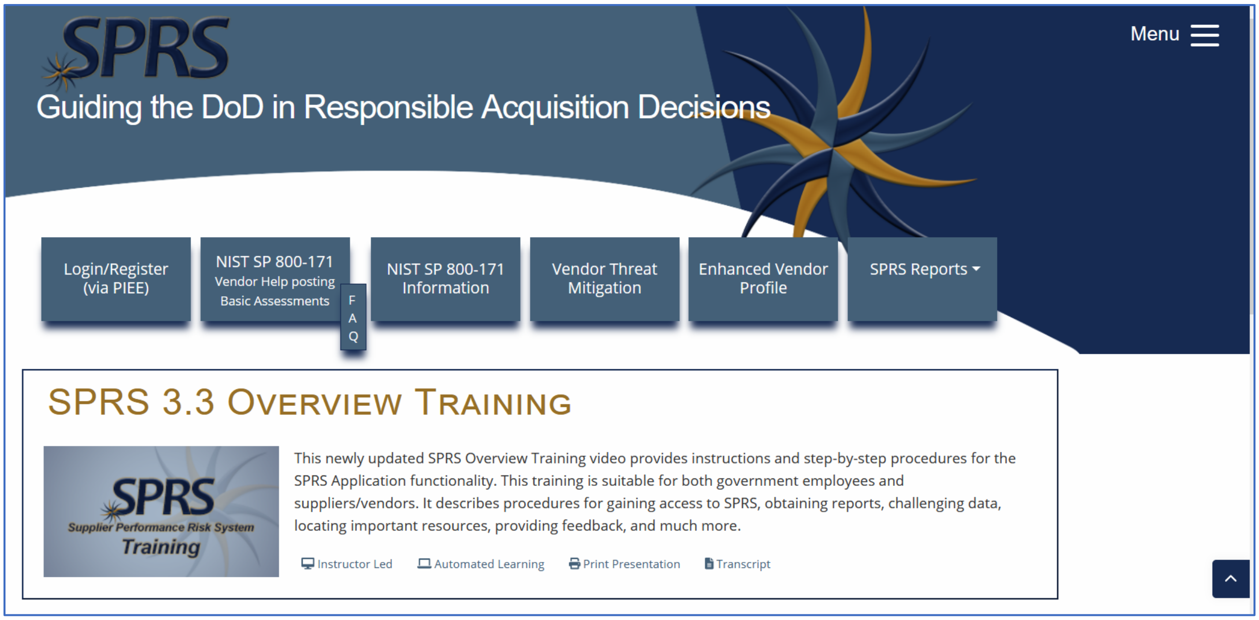
All DoD projects that will collect, transmit, or store CUI data must have a current Cyber Risk Management Plan (CRMP) IAW with NIST SP 800-171 and the DFARS CUI Guide.

Templates are provided for each of the documents and the IE and ESTCP offices will assist contractors/vendors to complete a CRMP. Note the templates can be used for both corporate IT business systems and OT FRCS projects. Typical CUI data on corporate IT systems includes design drawings and site information (CAD, BIM, GIS), specifications, test results, and consumption data (meter, site data). Typical CUI on OT projects includes network traffic (Modbus, BACNet, TCP/IP) between HMI and lower level controllers, configuration files, hardware/software versions and hashes, and consumption data (meter, site data).

The following documents are typically included in the CRMP (presented in order of recommended completion):

- CRMP Table of Contents Checklist
- Event/Incident Communications Plan (EICP)
- Event/Incident Response Plan (EIRP)
- Information Systems Contingency and CONOPS Plan (ISCP)
- Information System Policies and Procedures (ISPP)
- Security Audit Plan (SAP)
- System Security Plan (SSP)
- Security Monthly (or Quarterly)Assessment Report (SMAR)
- Plan of Action & Milestones (POAM)
- DFARS CUI DIBNet Incident Response Form
- US-CERT Incident Response Form
- CJCSM 6510.01B Incident Response Form

An organization completes the CRMP process by registering in the Supplier Performance Risk System (SPRS) and Self-Attesting they have a CRMP in place and an active Plan Of Action and Milestones (POAM) to track and mitigate vulnerabilities and risk as they arise (such as DHS CISA Alerts and Advisories, Emergency Directives, Vendor notifications, etc.).


SPRS
Guiding the DoD in Responsible Acquisition Decisions
Menu
Login/Register (via PIEE)
NIST SP 800-171 Vendor Help posting Basic Assessments
FAQ
NIST SP 800-171 Information
Vendor Threat Mitigation
Enhanced Vendor Profile
SPRS Reports
SPRS Supplier Performance Risk System Training
Instructor Led
Automated Learning
Print Presentation
Transcript

SPRS 3.3 Overview Training

This newly updated SPRS Overview Training video provides instructions and step-by-step procedures for the SPRS Application functionality. This training is suitable for both government employees and suppliers/vendors. It describes procedures for gaining access to SPRS, obtaining reports, challenging data, locating important resources, providing feedback, and much more.

Figure 14 – DoD Supplier Performance Risk System Website

Both Prime contractors and DoD Acquisition offices are now requiring a copy of an organization's Self-Attestation letter under CMMC1 as required by the DFARS 7020 clause.

> "(g) Subcontracts.
>
> **(1) The Contractor shall insert the substance of this clause, including this paragraph (g), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items (excluding COTS items).**
>
> (2) The Contractor shall not award a subcontract or other contractual instrument, that is subject to the implementation of NIST SP 800-171 security requirements, in accordance with DFARS clause 252.204-7012 of this contract, unless the subcontractor has completed, within the last 3 years, at least a Basic NIST SP 800-171 DoD Assessment, as described in https://www.acq.osd.mil/asda/dpc/cp/cyber/safeguarding.html#nistSP800171, for all covered contractor information systems relevant to its offer that are not part of an information technology service or system operated on behalf of the Government."

CMMC2 Final Rule Making is expected to be completed in 2023 and after that most large Primes and DIB Contractors will be required to undergo 3rd Party validation/certification.

SUMMARY

Cybersecuring control systems and contractor business systems that have CUI are an evolving practice but it is essential that organizations that hold the sensitive information on how the systems were designed, installed, commissioned, and operate have robust and state of the practice cyber hygiene in place. Loss of the information could result in a compromise of the systems and become a cyber incident that could result in physical destruction, loss of life or property, and direct mission impact. Industry and Organizations are becoming more cyber aware and training is available for Hunt and Defend, Cyber Incident Response, and protecting CUI.