



SAME NoVA & DC Posts Proudly Present:

Industry Government Engagement (IGE)

# IMPROVING CYBERSECURITY AND SAFETY IN SMART BUILDINGS AND INFRASTRUCTURE

Session III  
Thursday, April 21  
3:00 pm - 7:00 pm

Premier Sponsors:



Jacobs

Michael Baker  
INTERNATIONAL



PARSONS

SIEMENS



**Welcome!**

*SAME NoVA & DC Posts present IGE Session III (2 PDH\*) followed by Q&A with our expert panelists followed by in-person happy hour networking.*

## Leveraging the SAME Platform to Enhance the Nation's Cyber Protection

Federal cyber security standards are rapidly evolving to respond to the explosive growth of malware, ransomware, and even "killware" attacks spreading across all sectors of society. In response, federal engineers have turned to the AEC industry for collaboration and recommendations to enhance the planning, design, and protection of smart technologies in buildings and infrastructure. Additionally, federal and State agencies are developing policies and guidance for cyber protections in a full range of projects funded through the \$1.2 Trillion Infrastructure Investment and Jobs Act (IIJA).

In this third session of the SAME Industry-Government Engagement on Cyber Security, learn about the outcomes of our working group to

THANK YOU TO OUR EVENT SPONSORS

Premier Sponsors:



Featured Sponsor:





# *Society of American Military Engineers*

## *DC & NoVA Post*



## **Pledge of Allegiance**

**I Pledge Allegiance To The Flag,  
Of The United States of America,  
And To The Republic, For Which  
It Stands, One Nation Under God,  
Indivisible, With Liberty, And  
Justice For All**





*Society of American Military Engineers*  
*DC & NoVA Post*



## Today's Agenda

- 3:00 pm:** Check-in opens
- 3:30 pm:** Opening Comments: DC Post President: Joe Yates
- 3:40 pm:** Main Program: Brian May - Welcome, introductions, panel discussion, followed by Q&A
- 5:30 pm:** Happy Hour Networking
- 7:00 pm:** Event Concludes



*Society of American Military Engineers*



## Upcoming DC & NoVA Programs

- **May 10-12:** JETC in Aurora, CO
- **May 6<sup>th</sup> :** DC Post “First Friday” Virtual Lunchtime Session Kick-Off
- **May 26<sup>th</sup>:** DC Post Luncheon Program w/ DBIA Mid-Atlantic Chapter
- **June 2<sup>nd</sup>:** NoVA Post Joint Data Center Program with USA-CO & 7x24 Exchange DC Chapter @ Lost Rhino Brewing Company
- **June 3<sup>rd</sup> :** DC Post “First Friday” Virtual Lunchtime Session
- **June 23<sup>rd</sup>:** DC Post Joint Conference with ACEC/MW and CMAA
- **July 14<sup>th</sup>:** NoVA Post Annual Scholarship Golf Tournament @ Penderbrook Golf Club
- **July 21<sup>st</sup>:** DC Post TopGolf Summer Celebration



*Starts May 6<sup>th</sup>!*



SAME Washington DC Post Proudly Presents:

# FIRST FRIDAY LUNCHTIME LEARNING SESSIONS

First Friday every month  
12:00 pm - 1:00 pm ET  
MS Teams Virtual Platform  
Earn 1 PDH each session

**CALL FOR PRESENTATIONS**



# Save the Date 2022 Scholarship Golf Tournament

SAME NOVA Post's 22<sup>nd</sup> Anniversary Golf Tournament,  
Games, Raffle, Food/Drinks, and Networking



Society of  
**SAME**  
American Military Engineers



## **When:**

Thursday, July 14, 2022  
Shotgun start at 8:30am

## **Where:**

Penderbrook Golf Club  
3700 Golf Trail Lane, Fairfax, VA

## **Cost:**

\$160 per player  
\$80 for Active Duty Military/Gov't  
\$55 for lunch only

## **Who Should Attend:**

Everyone is welcome including  
retired and active duty  
military/government personnel.

***Registration Opening Soon!***

# Sponsorship Opportunities

## 2022 Scholarship Golf Tournament

SAME NOVA Post's 22<sup>nd</sup> Anniversary Golf Tournament, Games, Raffle, Food/Drinks, and Networking



Society of  
**SAME**  
American Military Engineers



All sponsorship packages will receive a wall certificate for their sponsorship and recognition during the awards ceremony.

### PLATINUM PACKAGE – \$3,000 each

- Company logo will be posted on SAME website with link to Company's website
- 2 Foursomes
- 1 Hole Sponsorship with Company Signage
- Opportunity to display marketing materials at hole of choice
- Logo displayed during August meeting networking time

### GOLD PACKAGE – \$2,000 each

- Company logo will be posted on SAME website with link to Company's website
- 1 Foursome
- 1 Hole Sponsorship with Company Signage
- Logo displayed during August meeting networking time

### SILVER PACKAGE – \$1,500 each

- Company logo will be posted on SAME website with link to Company's website
- 3 Players
- 1 Hole Sponsorship with Company Signage
- Logo displayed during August meeting networking time

### Additional Sponsorship Opportunities:

- LONGEST DRIVE / CLOSEST TO THE PIN / STRAIGHTEST DRIVE SPONSORS – \$500 each
- HOLE-IN-ONE SPONSOR – \$750  
*Win \$25,000 or a vehicle!*
- COURSE SPONSORS – \$250 each  
*Logo displayed on the course*
- BREAKFAST SPONSOR – \$250 each
- LUNCHEON SPONSOR – \$500 each
- BEVERAGE CART SPONSOR – \$500 each
- TROPHY SPONSOR – \$500  
*Sponsor will have the opportunity to hand out the award trophies at the ceremony.*

### Payment Information:

Make checks payable to "SAME NOVA Post" or use your credit card once registration opens.

### Mail payments to:

ATTN: George Guszczka, Michael Baker International  
3601 Eisenhower Ave, Suite 600  
Alexandria, VA 22304

### Questions?

Jenny Bowers: [Jenny.Bowers@exp.com](mailto:Jenny.Bowers@exp.com)  
or 703-397-4878



THANK YOU TO OUR EVENT SPONSORS

Premier Sponsors:



Featured Sponsor:





*Society of American Military Engineers  
DC & NoVA Post*



**Thank you for sticking with NoVA Post, DC Post, and SAME during these challenging times!**

**Please watch for emails, our Newsletter, social media posts, and check out our website for future events**

**<https://www.same.org/NOVA>**

**<https://www.same.org/DCPost>**



# Cybersecurity for Operational Technology

**Michael Dransfield**  
OT Cybersecurity SME  
NSA Cybersecurity Directorate  
**Ecton English**  
ICS Program Manager  
NSA Facilities Operations

**JOIN CYBERSECURITY ADVISORY**  
LAWRENCE  
April 13, 2012

### APT Cyber Tools Targeting ICS/SCADA Devices

**SUMMARY**  
The Department of Energy (DOE), the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), and the Federal Bureau of Investigation (FBI) are releasing this Joint Cybersecurity Advisory (JCA) to warn that certain advanced persistent threat (APT) actors have exhibited the capability to gain full system access to multiple industrial control systems (ICS)/supervisory control and data acquisition (SCADA) devices, including:

- Schneider Electric programmable logic controllers (PLCs),
- OMRON System NEX PLCs, and
- Open Platform Communications Unified Architecture (OPC UA) servers.

The APT actors have developed custom-made tools for targeting ICS/SCADA devices. The tools enable them to scan for, compromise, and control affected devices once they have established initial access to the operational technology (OT) network. Additionally, the actors can compromise Windows-based engineering workstations, which may be present in information technology (IT) or OT environments, using an exploit that compromises an ASRock motherboard driver with known vulnerabilities. By compromising

**Actions to Take Today to Protect ICS/SCADA Devices**

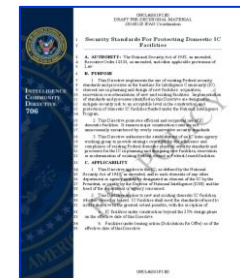
- Enforce multifactor authentication for all remote access to ICS networks and devices whenever possible.
- Change all passwords to ICS/SCADA devices and systems on a consistent schedule, especially all default passwords, to device-unique strong passwords to mitigate password brute force attacks, and to give defender monitoring systems opportunities to detect common attacks.
- Leverage a properly installed continuous OT monitoring solution to log and alert on malicious indicators and behaviors.

**National Security Agency Cybersecurity Advisory**  
Chinese State-Sponsored Actors Exploit Publicly Known Vulnerabilities in VBAT Communications

**Summary**  
Chinese state-sponsored actors have exploited publicly known vulnerabilities in VBAT communications to gain access to VBAT systems and data. The actors used a combination of publicly known vulnerabilities and custom-developed tools to compromise VBAT systems. The actors used a combination of publicly known vulnerabilities and custom-developed tools to compromise VBAT systems. The actors used a combination of publicly known vulnerabilities and custom-developed tools to compromise VBAT systems.


**Actions to Take Today to Protect VBAT Communications**

- Enforce multifactor authentication for all remote access to VBAT systems and devices whenever possible.
- Change all passwords to VBAT systems and systems on a consistent schedule, especially all default passwords, to device-unique strong passwords to mitigate password brute force attacks, and to give defender monitoring systems opportunities to detect common attacks.
- Leverage a properly installed continuous VBAT monitoring solution to log and alert on malicious indicators and behaviors.



# The Pathway to Success

How to do business with the National Security Agency:

- Visit our website: [www.nsa.gov/business/getting-started](http://www.nsa.gov/business/getting-started)
  - Register your company
    - SAM at [www.sam.gov](http://www.sam.gov)
    - NSA's Acquisition Resource Center at [www.nsaarc.net](http://www.nsaarc.net)
  - Register to attend one of our Pathway To Success briefings via the ARC or via the getting started page
  - Network!
    - Networking with industry is likely more important than with the government
    - Business In A Minute – Agency event to meet with prime contractors and government representatives
- 





# PROTECTING CRITICAL INFRASTRUCTURE

*Cybersecurity Threats and the Need for Action*

APRIL 21, 2022

# CYBERSECURITY THREATS TO CRITICAL INFRASTRUCTURE

## INCREASING ATTACKS



Recent high-profile attacks have **increased in sophistication and malice**

Expanding attack surface is introducing new operational challenges and risks.

Growing **black/dark web** market for ICS or 'SCADA access-as-a-service' and other tools

Ransomware infections on ICS to be **more frequent and severe**

## COMPLEXITY



While many physical devices are **common, individual implementation is unique** to the process being controlled

Enhanced features on newer ICS devices **increases attack surface** and likelihood of vulnerabilities

Large volume of legacy equipment and proprietary protocols require a **lower level of sophistication for an attacker to succeed**

## MISSION DRIVERS



Attacks have **increased operational recognition** of risks to mission and readiness

Leaders want **real-time access** into the process data, leading to **increased interconnectivity**

Finding individuals versed in **industrial engineering and cybersecurity**, is increasingly challenging



WEAPONS PLATFORMS  
*(Non-exhaustive)*



LOGISTICS AND DISTRIBUTION CENTERS



AIRFIELD SYSTEMS



ELECTRONIC SECURITY SYSTEMS



FUELING SYSTEMS



FACILITY RELATED CONTROL SYSTEMS (FRCS)

## CYBERSECURITY THREATS TO CRITICAL INFRASTRUCTURE

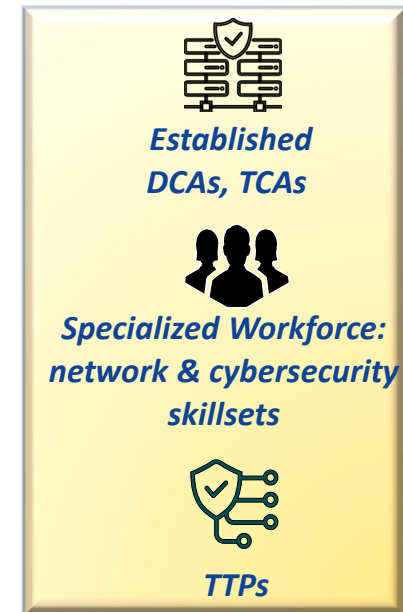
**The 2022 NDAA emphasizes *Critical Infrastructure Cybersecurity*. Section 1505** calls out Operational Technology and Mission-relevant Terrain in Cyberspace. Objectives are intended for the public sector. ***Where do we begin?***



The bridge from NDAA to execution is built on the Services & lower echelons (AOs, engineers)

- Governance, dedicated resources, oversight
- Team sport – starts with mission, people, priorities, culture
- Not just a compliance problem, but a readiness issue

- DoD/Service strategies emphasize fundamental actions now to ensure mission cybersecurity
  - Clear specifications and performance guidance for cyber protection of smart IT/OT
  - Understanding of external dependencies (power, gas, water) inside and beyond the fence-line
  - Asset inventories - what OT systems do we have now? Prioritize crown jewels/critical assets
- Technology & digital innovation is a top priority for OT cybersecurity – Securing Physical Systems & Processes
  - Integration is paramount – watch out for too many technologies, need to align and integrate
  - holistic approach supports cyber “defense-in-depth” – integration from “sensor-to-SCADA”
  - Need to have standards & synchronization
- The future is going to Zero Trust and it’s moving fast - NDAA Section 1528
  - Networks more interconnected – asset owners need visibility
  - Emphasizes security, least privilege, continuous monitoring





# Cyber IGE PT Update



April 21, 2022



# Agenda

- **IGE Charter Review**
- **White Paper Status**
- **Way Ahead**

# IGE Charter

## 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

Proposed updates to targeted documents, starting with specifications (UFGS) and criteria (UFCs) related to Control System Cybersecurity UFC (UFC 4-010-06) and UFGS (UFGS 25 10 10) as well as of the UFCs and UFGS for HVAC controls and Utility Monitoring and Control Systems.

# IGE Charter

## Deliverable:

- ❑ **White Paper on Reducing Cyber Risk in Smart OT for Federal Facilities and Infrastructure**
  - **Discuss risks associated with use of smart OT in federal facilities (awareness, thought leadership)**
  - **Discuss potential cyber risk mitigation strategies (awareness, thought leadership)**
  - **Curated list of best practices for securing smart OT for federal facilities and infrastructure (awareness)**
  - **Proposed framework for analyzing risk and the criticality of mitigating vulnerabilities (awareness, advocacy)**
  - **Design review checklist for protection of smart building management systems. (awareness)**
  - **Recommended changes to applicable policies and specifications as informed by best practices (advocacy)**

# White Paper Content

UFC 4-010-06  
19 September 2016  
Change 1, 18 January 2017

## UNIFIED FACILITIES CRITERIA (UFC)

### CYBERSECURITY OF FACILITY-RELATED CONTROL SYSTEMS



APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

.....  
USACE / NAVFAC / AFCEC / NASA UFCS-25 10 10 (February 2019)  
Change 1 - 09/21  
.....  
Preparing Activity: USACE Superseding  
UFCS-25 10 10 (November 2015)

UNIFIED FACILITIES GUIDE SPECIFICATIONS

References are in agreement with USML dated October 2021  
.....

SECTION TABLE OF CONTENTS

DIVISION 25 - INTEGRATED AUTOMATION

SECTION 25 10 10

UTILITY MONITORING AND CONTROL SYSTEM (UMCS) FRONT END AND INTEGRATION

02/19, CRG 1: 05/21

PART 1 GENERAL

1.1 SUMMARY

1.1.1 System Requirements

1.1.1.1 General System Requirements

1.1.1.2 LonWorks Requirements

1.1.1.3 BACnet Requirements

1.1.1.4 Modbus Requirements

1.1.1.5 OPC Requirements

1.1.1.6 Niagara Framework Requirements

1.1.2 Symbols, Definition and Abbreviations

1.1.3 System Units and Accuracy

1.1.4 Data Packages/Submittals Requirements

1.2 RELATED SECTIONS

1.3 REFERENCES

1.4 DEFINITIONS

1.4.1 Alarm Generation

1.4.2 Alarm Handling

1.4.3 Alarm Routing

1.4.4 Application Generic Controller (AGC)(LonWorks)

1.4.5 Application Specific Controller (ASC)(LonWorks)

1.4.6 BACnet (BACnet)

1.4.7 BACnet Advanced Application Controller (B-AAC)(BACnet)

1.4.8 BACnet Advanced Operator Workstation (B-AOS)(BACnet)

1.4.9 BACnet Application Specific Controller (B-ASC)(BACnet)

1.4.10 BACnet Building Controller (B-BC)(BACnet)

1.4.11 BACnet Internetwork (BACnet)

1.4.12 BACnet Interoperability Building Blocks (BIBBs) (BACnet)

1.4.13 BACnet Operator Display (B-OD)(BACnet)

1.4.14 BACnet Operator Workstation (B-OWS)(BACnet)

1.4.15 BACnet Smart Actuator (B-SA)(BACnet)

1.4.16 BACnet Smart Sensor (B-SS)(BACnet)

1.4.17 BACnet Testing Laboratories (BTL) (BACnet)

1.4.18 BACnet Testing Laboratories (BTL) Listed (BACnet)

SECTION 25 10 10 Page 1



## Department of Defense INSTRUCTION

NUMBER 8510.01  
March 12, 2014  
Incorporating Change 3, December 29, 2020  
DoD CIO

SUBJECT: Risk Management Framework (RMF) for DoD Information Technology (IT)

References: See Enclosure 1

### 1. PURPOSE. This instruction:

- a. Reissues and renames DoD Instruction (DoDI) 8510.01 (Reference (a)) in accordance with the authority in DoD Directive (DoDD) 5144.02 (Reference (b)).
- b. Implements References (c) through (f) by establishing the RMF for DoD IT (referred to in this instruction as "the RMF"), establishing associated cybersecurity policy, and assigning responsibilities for executing and maintaining the RMF. The RMF replaces the DoD Information Assurance Certification and Accreditation Process (DIACAP) and manages the life-cycle cybersecurity risk to DoD IT in accordance with References (g) through (k).
- c. Redesignates the DIACAP Technical Advisory Group (TAG) as the RMF TAG.
- d. Directs visibility of authorization documentation and reuse of artifacts between and among DoD Components deploying and receiving DoD IT.
- e. Provides procedural guidance for the reciprocal acceptance of authorization decisions and artifacts within DoD, and between DoD and other Federal departments and agencies, for the authorization and connection of information systems (ISs).

### 2. APPLICABILITY

- a. This instruction applies to:
  - (1) OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff (CJCS) and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense (OIG DoD), the Defense Agencies, the DoD Field Activities, and



## DEPARTMENT OF DEFENSE CONTROL SYSTEMS SECURITY REQUIREMENTS GUIDE

Version 1, Release 1

January 26, 2021

1

FRCS UFC: <https://www.wbdg.org/ffc/dod/unified-facilities-criteria-ufc/ufc-4-010-06>

UMCS FRGS: <https://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-25-10-10>

DODI 8510.01: <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001p.pdf?ver=2019-02-26-101520-300>

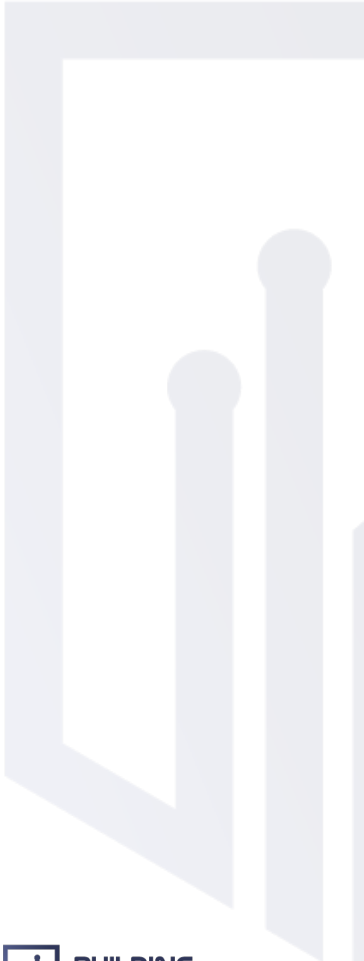
DoD CSSRG: [https://dl.dod.cyber.mil/wp-content/uploads/external/pdf/Jan\\_26\\_Control\\_Systems\\_SRG.pdf](https://dl.dod.cyber.mil/wp-content/uploads/external/pdf/Jan_26_Control_Systems_SRG.pdf)





# White Paper Roles

IGE White Paper Content Area	Content Lead	Content Support	Content Support
1. Risks associated with use of smart OT in federal facilities	Susan Howard	Fred Gordy	Marianne Meins
		Bob Murphy	Ali Elnaamani
		Daryl Haegley	
		Wanda Lenkevich	Michelle Sipe Exaros
2. Potential cyber risk mitigation strategies	Dave Forbes	Bob Murphy	Michael Chipley
			Ali Elnaamani
3. Curated list of best practices for securing smart OT for federal facilities and infrastructure		Dave Forbes	
		Bob Murphy	
		Marianne Meins	
4. Proposed framework for analyzing risk and the criticality of mitigating vulnerabilities	Bob Murphy		
5. Design review checklist for protection of smart building management systems	Susan Howard	Bob Murphy	Michael Chipley
		Wanda Lenkevich	David Brearley
		Marianne Meins	
6. Recommended changes to applicable policies, criteria, & specs as informed by best practices	Chris Schmidt	Fred Gordy	David Brearley
		Bob Murphy	
		Michelle Sipe Exaros	



# White Paper Content

**Problem Statement / Context**

**Content Area 1**

**Background / Analysis**

**Content Areas 2 & 3**

**Recommendations/Checklist for Designers**

**Content Areas 4, 5, & 6**

**Simplified, Actionable Guidance for Planners,  
Designers and Operators of Federal Facilities**

# IGE Milestones

- ✓ **Kickoff Panel – DC/NoVA Post Meeting – 16 Sep 2021**
- ✓ **Charter approved and IGE Working Group established Oct 20, 2021**
- ✓ **Commencement of IGE activities – Oct 26, 2021**
- ✓ **Vector Check – SBC CEO Roundtable – Nov 2021**
- ✓ **Establish Teams/SharePoint Sites**
- ✓ **Process Team Meeting – 25 Jan 2022**
- PT Progress Update – DC/Nova Post – 21 Apr 2022**
- PT Status Update to SAME Executive Committee – JETC – May 2022**
- Draft White Paper Content Due – 31 May 2022**
- PT Working Sessions/Develop Draft White Paper – Jun – Aug 2022**
- Draft White Paper Revisions – Sep 2022**
- Present White Paper at CEO Roundtable – SBC – Nov 2022**

# 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.



**BUILDING**  
Cyber Security



Questions?

