Society of SAME American Military Engineers

NoVA Northern Virginia Post

SAVE THE DATE

- **Nov 7** – Young Professional Happy Hour – Bull Run Winery
- **Nov 20-22** – SAME National Small Business Conference, New Orleans
- **Dec 5** – SAME NOVA Post – MWAA Briefing at Army Navy Club Arlington
- **Dec 6** – SAME DC & NOVA Post – 2024 Leadership and Mentoring Graduation
- **Dec 14** – SAME DC & NOVA Post – Wreath Laying at Arlington Cemetery

www.same.org/nova

Society of SAME American Military Engineers

NoVA Northern Virginia Post

Todays Program is moderated by Lucian Niemeyer:

1110 – 1200: IGE Update with Tom Barley and Wanda Lenkewich

1200-1225: Fireside Chat with Daryl Haegley on the USAF perspective and way forward on OT Cyber

1225 – 1255: Fireside Chat with Lori Jackson – Update on CMMC

1255: Q&A/Closing

We will use the CHAT feature to post Questions during the briefing

This Briefing is UNCLASSIFIED

Society of SAME American Military Engineers

AMERICAN MILITARY ENGINEERS

NoVA Northern Virginia Post

GUEST SPEAKER & Moderator

Mr. Lucian Niemeyer, F. SAME

CEO, Building Cyber Security

Lucian serves as the Chief Executive Officer of Building Cyber Security, a private sector, non-profit organization enhancing global safety through the development of cyber security protections for intelligent technologies, buildings and communities. In this role, he applies his expertise and experience to the nexus of facilities, real estate, and technology to mitigate the risk and impacts to society from the growing threat of cyber incidents.

Over three decades, Lucian has served in the White House, the Pentagon, and in Congress providing budget, policy, and management leadership for U.S. national security programs. The Honorable Niemeyer served as an Assistant Secretary of Defense managing the world's largest real property portfolio valued at a trillion dollars. Lucian also served the Secretary of Defense as a strategic advisor for critical mission assurance and cybersecurity programs, as an Assistant Secretary of the Navy, and in the Office of Management and Budget at the White House overseeing national security, nuclear, and intelligence programs.

Lucian is an Air Force veteran with 21 years of active and Virginia Air National Guard service. He holds a Bachelor of Architecture, from the University of Notre Dame, a Master of Business Administration from The George Washington University, and a Master of National Security and Strategic Studies from the Naval War College. He is a Fellow in the Society of American Military Engineers, a member of the National Academy of Construction, is an Honorary Seabee, and actively promotes Standards of Care for cyber safety in the engineering profession

BUILDING Cyber Security

Enhancing Cyber Protections

A SAME Industry/Government Engagement

www.buildingcybersecurity.org

Society of SAME American Military Engineers

Nov 2024

Learning Objectives

- Understand the growing cyber risk to connected, automated building systems and other technologies
- Apply emerging cyber engineering and construction practices, to enhance building safety
- Analyze the value to building owners and customers of offering expertise in building system cyber safety and security during construction
- Evaluate recently developed cyber safety and security performance frameworks to augment federal guidance

Update of Progress of the Cyber SAME IGE

Line- Up

- 11:00- 11:10 am – Introduction by Lucian
- 11:10 – 12:00 pm - IGE Update with Tom Barley and Wanda Lenkewich
- 12pm - 12:25 - Chat with Daryl Haegley with the AF perspective and way forward on OT cyber
- 12:25- 12:55 pm - Update on CCMC - Chat with Lori Jackson
- 12:55 close

Please Submit Questions to Chat

Feb 7, 2024 – Joint Cybersecurity Advisory

"The **People's Republic of China (PRC)** state-sponsored cyber actors are seeking to pre-position themselves for disruptive or destructive cyberattacks against U.S. critical infrastructure in the event of a major crisis or conflict with the United States."

"Confirmed that Volt Typhoon has compromised the IT environments of multiple critical infrastructure organizations—primarily in **Communications, Energy, Transportation Systems, and Water and Wastewater Systems Sectors**."

"**Critical infrastructure organizations** are urged to apply the mitigations in this advisory and to hunt for similar malicious activity."

What the Experts Said in Congressional Testimony

FBI Director Chris Wray - "China's hackers are positioning on American infrastructure in preparation to wreak havoc and cause real-world harm to American citizens and communities, if or when China decides the time has come to strike.. Let's be clear: Cyber threats to our critical infrastructure represent real world threats to our physical safety."

CISA Director Jen Easterly - "Imagine not one pipeline, but many pipelines disrupted and telecommunications going down so people can't use their cell phone. People start getting sick from polluted water. Trains get derailed. Air traffic and port control systems are malfunctioning,"

Chairman Mike Gallagher - We are no longer discussing hypotheticals – China's action, "is the cyberspace equivalent of placing bombs on American bridges, water treatment facilities, and power plants. There is no economic benefit for these actions. There is no intelligence gathering rationale. The sole purpose is to be ready to destroy American infrastructure, which will inevitably result in mass American casualties."

SAME 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.

- https://www.wbdg.org/ffc/dod/unified-facilities-criteria-ufc/ufc-4-010-06
- https://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-25-10-10

BUILDING Cyber Security

Recommendations

- **A/E/C Industry Recognizing Need to Engineer Cyber Safety into Projects**
  - **Firewalls/airgaps are not the answer in an IT/OT convergence**
  - **Collaboration between network and facility designers/engineers on specifications, configuration instructions, submittal reviews, and cyber commissioning requirements**
  - **Using digital twinning and baseline building system performance metrics as the next generation of as-builts for smart technologies**
  - **Specifying new types of data transport architecture to be able to monitor smart technologies (ie Fiber to the edge)**
  - **A/E/C needs to partner with cyber security firms offering OT protection capabilities**
  - **Federal Facility engineers would benefit from OT cyber incident training**
  - **Division 25 must be updated to account for smart building automation and cyber**

A/E/C Firms are joining BCS to access cyber safety expertise for development of a cyber practice and the offer of a "Technologist of Record" for buildings and infrastructure

BUILDING Cyber Security

Panel 1

Wanda Lenkewich , PE, CxA, LEED AP

Founder and CEO Chinook Systems, Inc.

Tom Barley, P.E., CISSP, PMP

FRCS Program Manager for Infrastructure Modernization & Resilience, Office of the Assistant Secretary of Defense for Energy, Installations and Environment (ASD(EI&E))

Getting Back to the Reqirements

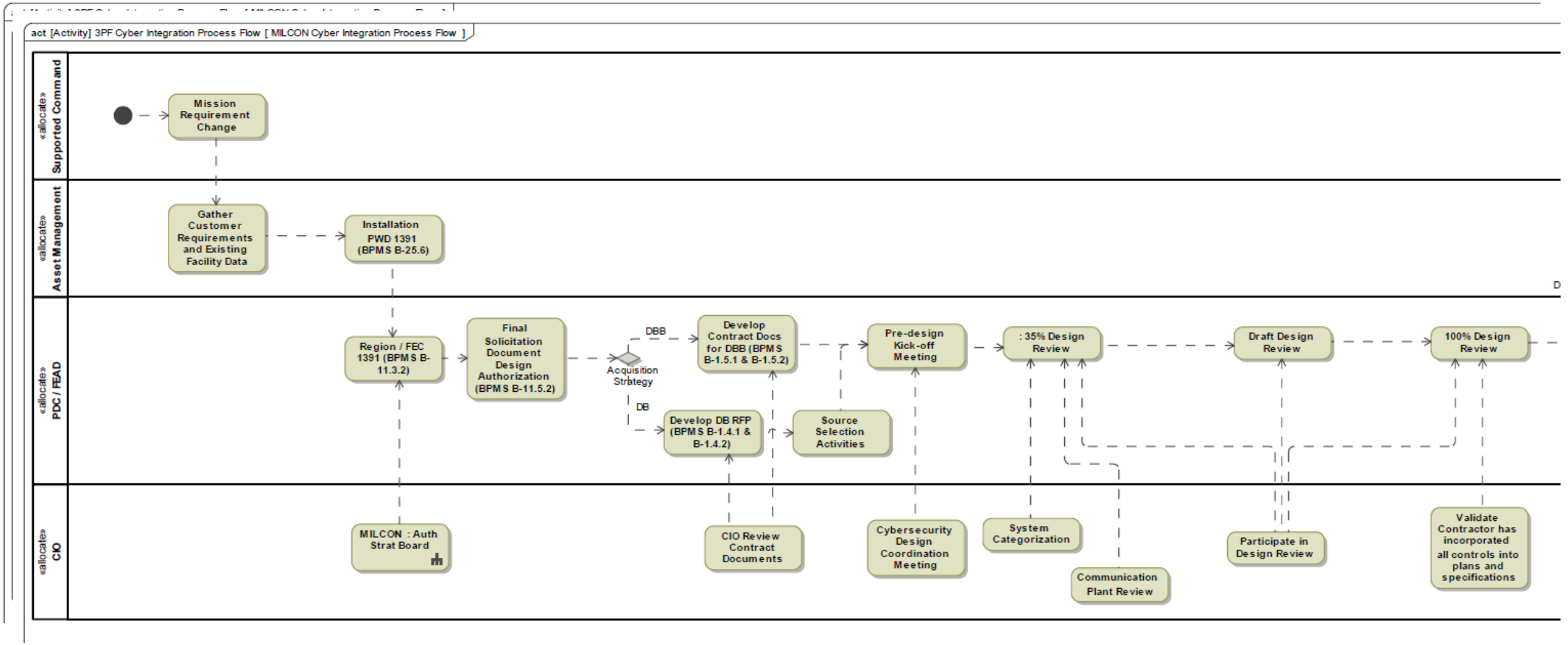
- OSD has led workshops bringing together all DOD Services & INDUSTRY relative to FRCS Cybersecurity Commissioning Requirements
- Purpose has been to identify minimum set of Facility Related Control Systems Cybersecurity requirements to be collected from Project “Owner & Operator” during initial Planning & Design processes
- This will form the basis for effective execution of UFC 4-010-006 “Cybersecurity of FRCS” and Cybersecurity Commissioning across DoD

Cybersecurity Module for 1391 Database

- **How do we get to better estimating of Cybersecurity for FRCS on MILCON Projects across DoD**

Index	Data Required	Proj/Syst	Field Type	Reference
1	Number of Systems	Per Project	Number	Systems per Project
2	System Type	Per System	Drop Down	FRCS Master List
3	Cybersecurity Strategy	Per System	Drop Down	Service Specific (MFR/ATO/etc)
4	Mission Impact	Per System	Drop Down	Mission Essential / Mission Support / Mission Critical
5	Mission Owner	Per System	Drop Down	Related to Mission Impact / Service Specific
6	Network Connection	Per System	Drop Down	Service Specific (Enclave + eMASS ID / None)
7	System Interconnection	Per System	Fill in Blank	eMASS ID / Nothing / System Type ~30 characters
8	Impact Rating	Per System	Drop Down	NIST RMF C-I-A (all 27)
9	System Owner	Per System	Drop Down	Service Specific
10	Notes	Per System	Fill in Blank	Fill in the blank, Paragraph, ~3,000 characters

Cyber Integration for Design



BUILDING Cyber Security

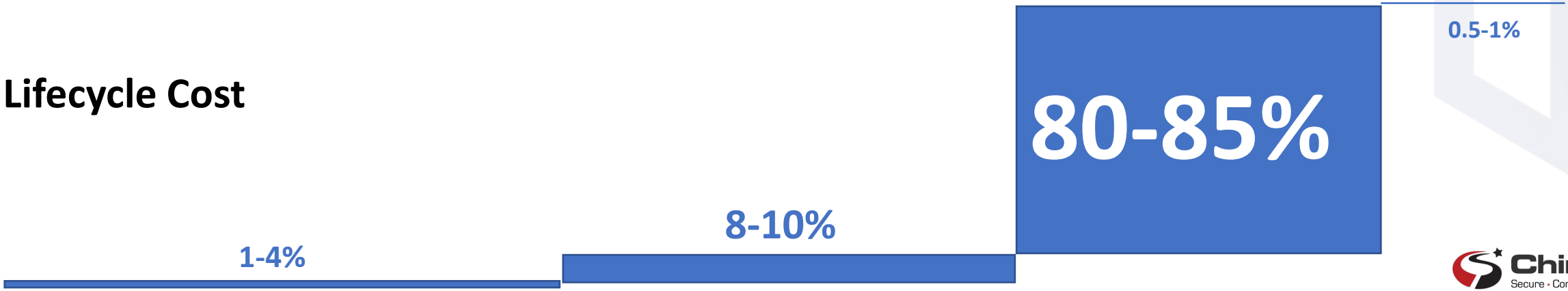
Status of UFGS and UFC

- A review of UFGS and UFC was conducted against the industry proposed Division 01 specification
- Crosswalk was conducted by the Government and current UFC/UFGS are being updated to incorporate gaps
- There is still work to be done to standardize process and resolve the knowledge and experience gap required to better deliver cyber commissioning during construction phase including but not limited to the alignment of the RMF process, better integration of cyber deliverables and activities during construction, and better transition (i.e. 1354s) into continuous monitoring of cybersecure systems

Integrating Cyber Commissioning into the Lifecycle

Acquisition, Planning and Design			Construction and Transition			Operations		Disposal
Budget, Funding Documents, Basis of Design	35% - 65% -95% Concept and Detailed Design	100% IFC	Product approval and Installation	Startup, Testing, and Validation	Transition	PM, Analytics, Monitoring	Repairs and Replacements	Decommission
OPR to incorporate Cyber Requirements	Focused review controls network design, hardware and software inventory	Formalize a plan for delivery of cyber activities	Equipment/ Device reviews, Acceptance checklists	Harden systems and devices before Cx Performance Testing	Systems Manuals to incorporate procedures to recover from an attack	Implement continuous monitoring for both internal and external threats	Reduce existing vulnerabilities or prevent potential new vulnerabilities	Ensure deletion of stored information
← 1-3 Years →			← 1-5 Years →			← 40-50 Years →		← 0-1 Years →

Lifecycle Cost



Chinook
Secure · Compliant · Efficient

Integration of Cx in Planning - OPR

Owner's Project Requirements (OPR) is a written document that details the functional requirements of a project **and the expectations of how it will be used and operated**.

This includes project and design goals, measurable performance criteria, budgets, schedules, success criteria, owner's directives, and supporting information.

The OPR must be developed with significant owner input and ultimate approval

[Resources | BCxA Building Commissioning Association]

Table of Contents

FRCS Cybersecurity

Chinook
Secure · Compliant · Efficient

Integration of Cx in Transition – Systems Manuals

The Systems Manual is an addition to the O&M Manuals submitted by the contractor and contains information not normally contained in the submitted O&M manuals.

The Systems Manual focuses on operating, rather than maintaining the equipment.

[1.10.5 Systems Manual Template Example Univ. Lab | BCxA Building Commissioning Association]

1. Overview
2. Design Record— HVAC / Electrical / Fire Alarm / Other
3. Sequences of Operation and Control Drawings
4. Shutdown for Maintenance & Manual Operation Procedures
5. Energy Related User Adjustable Set Points & Reset Schedules
6. Recalibration & Recommissioning Frequencies Procedures.
7. Energy Tracking Guidelines.
8. Diagnostic Trend Logs
9. Energy Alerts
10. Notes to the Operator
11. User Manual

FRCS Cybersecurity

Chinook
Secure · Compliant · Efficient

Warfighting Seminar

Learning Objectives for Mission Recovery from a Cyber Attack to a Military Critical Asset

- Review processes to **identify** the critical systems and cyber vulnerabilities in a critical asset within a risk management framework
- Identify proactive measures to **protect** critical systems and mitigate risk of a cyber attack
- Present methods to **detect and confirm** the origin and method of a cyber attack to a critical system as well as extent of damage
- Develop checklists and protocols for military engineers to quickly **isolate, respond and communicate progress** to the incident
- Assess options, probabilities and timing for the **recovery** of the missional essential system
- Identify programs to quickly share information within DOD and others on the source and methods for the incident

The scenario includes input from building system manufacturers, facility designers, facility operators, and cyber security experts

BUILDING Cyber Security

SAME IGE Future Activities

Continued Collaboration on Updated Cyber Safety

- ❑ Augmenting UFC with specific specifications
- ❑ Targeting Whole Building Design Guide and DOD guidance

Small Business Conference 2024 – New Orleans November 20-22

- ❑ Small Business Round Table for cyber services
- ❑ Technical Review Session for Small Businesses and USACE/NAVFAC on use of cyber safety specification
- ❑ Cyber IGE Training Working Group for Federal Engineers and Public Works Personnel
- ❑ Cyber IGE Facility Management Working Group

BUILDING Cyber Security

Panel 2

Daryl Haegley, GICSP, OCP

Technical Director, Control Systems Cyber Resiliency U.S. Department of the Air Force

Responsibilities include providing technical oversight for world-wide operations of Air and Space Force objectives in cybersecurity, defense, and resiliency for infrastructure and control systems. In addition, he provides direction and recommended action to the Deputy Chief of Staff of Logistics, Engineering, & Force Protection on matters pertaining to formulation, review, and execution of plans, policies, and programs related to all Control Systems activities in the DAF.

Haegley's distinguished career includes more than 30 years of military, federal, civilian, and commercial consulting experience. For over a decade, Mr. Haegley has become easily recognized as the leading champion in bringing awareness to the ever-increasing cyber threat to control systems and his unprecedented leadership resulted in measurable changes in government and industry.

He has four certifications, three Masters degrees, two children, and one patent.

Achieve Effects in Space via Ground OT

2023

Gen. B. Chance Saltzman, Chief of Space Operations, U.S. Space Force

Ukraine situation:

- **One of Russia's earliest endeavors was to deny Ukrainian troops access to a satellite comms system (Viasat) stationed in geosynchronous orbit**
- **"And they did it with a cyber attack against the ground infrastructure … so you attack the ground network to achieve the space effect you want"**

Takeaway:

- **If adversary believes it cannot achieve military objective, it will hesitate to "cross a threshold of violence." No conflicts. No debris. No crisis.**

OT System Owners: Critical to Mission!!

Cyberattacks on Guam Could Disrupt Indo-Pacific US Forces

Key Indo-Pacific outpost for US forces & potential conflict location between US and China
- Logistics & munitions hub
- Intelligence, surveillance & reconnaissance node

- Successful Chinese **cyberattacks on critical infrastructure in Indo-Pacific** footholds could **cripple US regional military capabilities**
- Beijing prepared to unleash cyberattacks on critical infrastructure and defense networks are meant to **cause confusion, divert resources, and disrupt military mobilization**
- **Volt Typhoon** intrusion detected in Guam – **snuck past digital defenses**
- Shift toward **targeting critical infrastructure shows eagerness to sabotage**
  - "**no economic value** in pre-positioning on oil and gas pipelines or water utility companies – there's **no intellectual property to steal.**" – Rep. Mike Gallagher

"[Cyberattacks on critical infrastructure] is **not an episodic threat** that we're going to face. **This is persistent.**"

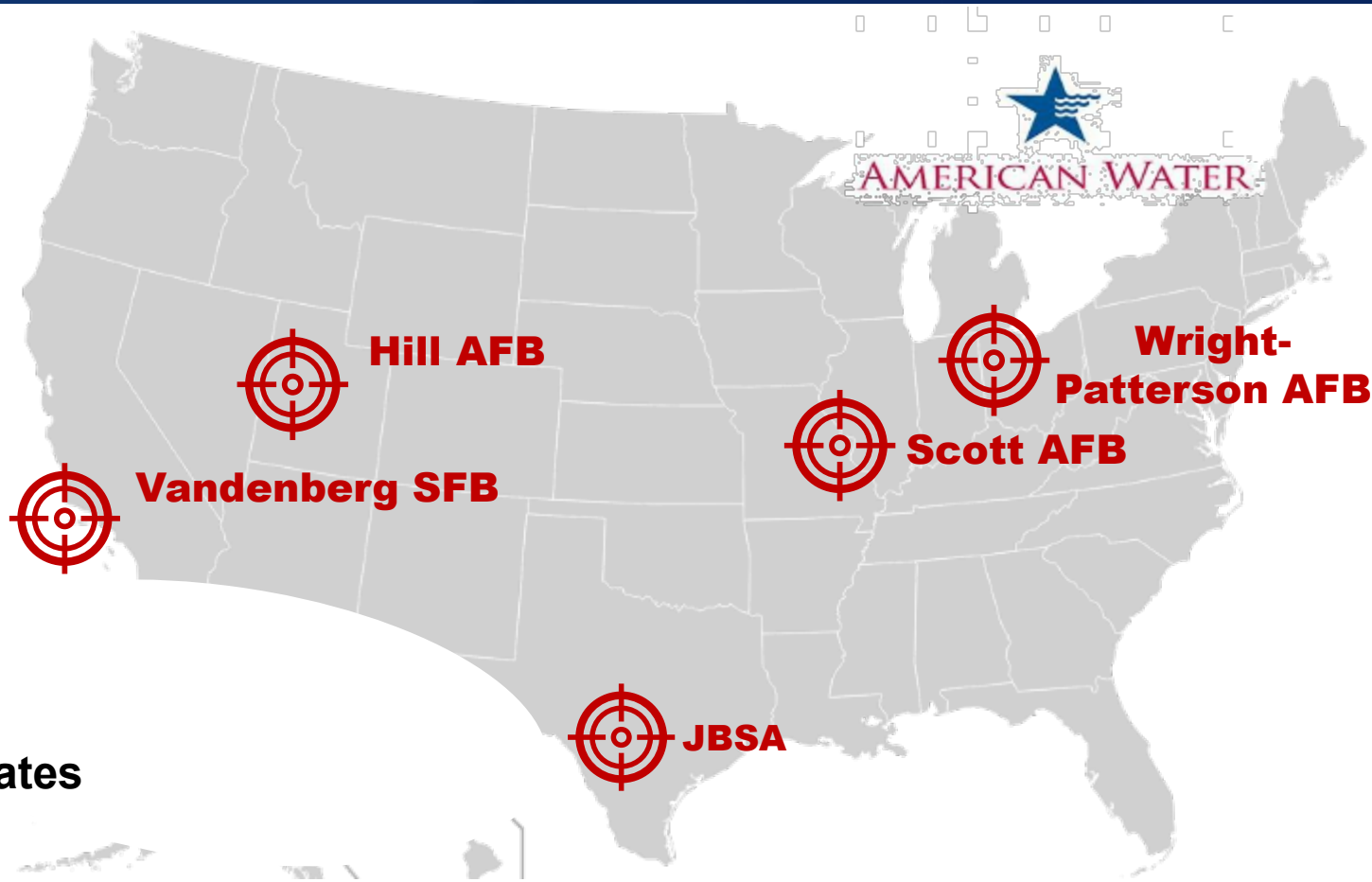
General Paul M. Nakasone
Director, NSA & Commander, USCYBERCOM

USCYBERCOM Does NOT DO OT Cyber Defense

In the News: American Water Cybersecurity Attack (Oct '24)

BLUF: 07 Oct '24 -largest water and wastewater utility company in US, American Water (AW), announced that it was victim of a cyberattack

- **Cyberattack against AW billing systems, halting operations for a week**
- **AW services 18 military sites including five DAF installations →**
- **Thankfully, no direct impact to water or wastewater services but attack demonstrates vulnerability in critical infrastructure**



Water and wastewater systems will continue to be vulnerable target for adversaries; Need increased focus / resources on water resiliency

Mar'21

DAF Strategic Plan for Control Systems

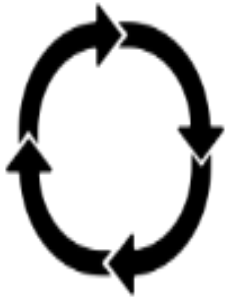
Prescribes direction, milestones, organizational responsibilities for establishing DAF-wide capabilities to both cyber-secure & cyber-defend critical control systems

100 Tasks
>$100Ms needed

4 LOEs:

Org Constructs & Workforce

Prioritization & Visibility



Lifecycle Resilience

Defense & Recovery

NDAA 1650 revealed inadequate DAF posture to address threat; DAF needed holistic strategy & implementation plan beyond Civil Engineering

Oct'24

Cyber Resiliency Office for Control Systems

Who:

CROCS

New office dedicated to coordinating & overseeing cyber defense & resilience of DAF OT/CS

What: <1 stop shop>

- Coordinate Policy among control system owners
- Coordinate between system owners and cyber defenders
- Oversight of DAF-wide DCI cyber initiatives
- Funding advocacy & spend priorities

Go BEYOND

Why:

Installations are power projection platforms underpinned by critical control systems / OT that expose critical assets to adversarial threats

Discussion…


RAMIREZ
LAS VEGAS REVIEW-JOURNAL
2024© CREATORS.COM
That PAGER ATTACK was A REAL EYE-OPENER.
IMAGINE if OUR SOFTWARE, HARDWARE and ELECTRONIC COMPONENTS WERE ALL MADE BY OUR ADVERSARIES...
iPhone16
NEW from CHINA

Panel 3

Lori Jackson
President and Senior Cybersecurity Engineer at White Raven Security

lori@whiteravensecurity.com

Lori has over 20 years of technical and management experience in cybersecurity compliance, cyber engineering, and corporate governance. Lori has spent her entire career committed to U.S. Defense through supporting small DIB contractors. Over the past several years, she has worked with companies to prepare their systems for NIST and CMMC compliance. Lori is a Certified Information Systems Security Professional (CISSP), CMMC Certified Assessor (CCA), CMMC Certified Professional (CCP), and a Registered Practitioner (RP). She serves as the SAME Resilience Community of Interest Vice Chair for Cyber. Lori is well-versed in U.S. Government cybersecurity policies and standards, with extensive experience designing systems to comply with UFC 4-010-06, NIST SP 800-171, the Risk Management Framework (RMF), and the Cybersecurity Maturity Model Certification (CMMC). Lori serves as Cybersecurity Engineer on Architect-Engineer (A-E) teams and has designed the Facility Related Control System (FRCS) cybersecurity according to UFC 4-010-06 for over 30 designs.

Interested in the Cyber IGE?

Contact

Lucian Niemeyer, F. SAME
Lucian@buildingcybersecurity.org

Open to Individuals and Companies

Society of SAME American Military Engineers

NoVA Northern Virginia Post

THANK YOU FOR YOUR CONTINUED SUPPORT!

Please watch for emails, Post Newsletter, Social media posts!
Check out our website for future events

This presentation will be uploaded to the NOVA Post website

www.same.org/NOVA

Special thanks today to:

- Mr. Lucian Niemeyer, F. SAME
  Building Cyber Security
- Ms. Lori Jackson, CISSP
  White Raven Security
- Ms. Wanda Lenkewich, PE
  Chinook Systems, Inc.
- Mr. Daryl Hegley GICSP, OCP
  US Air Force
- Tom Barley, PE
  OSD (EI&E)

Society of SAME American Military Engineers

NoVA Northern Virginia Post

SPECIAL THANKS TO OUR
2024 ANNUAL SPONSORS

Actalent
Axias BUILDING VALUE
Dewberry
ECS
MERRICK
RCS
Schnabel ENGINEERING
Sorba ENGINEERING
Stantec
SZ PM Consultants, Inc.
TERRA CONSTRUCTS Buildings & Infrastructure
WOODS · PEACOCK ENGINEERING CONSULTANTS
wsp