WARFIGHTER SEMINAR SERIES

Mission Recovery from a Cyber Physical System Attack on a Domestic National Security Asset

May 2, 2023, 1:00 p.m.

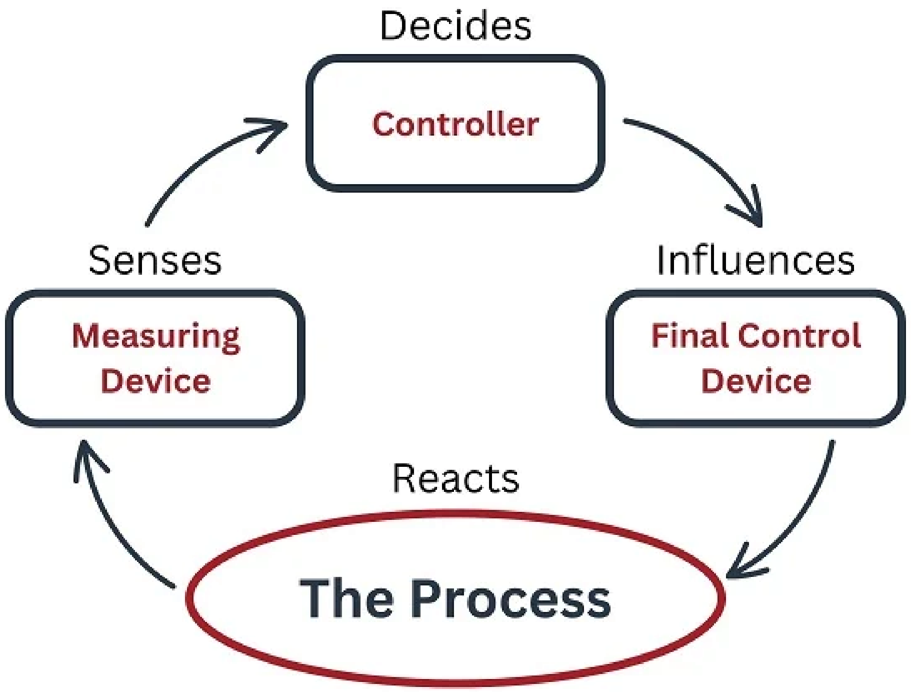
OPENING REMARKS

OPERATIONAL TECHNOLOGY (OT) CYBERSECURITY

PROTECTING MISSION READINESS

OT includes Industrial Control Systems (ICS), Supervisory Control And Data Acquisition (SCADA) systems, security systems, Uncrewed Vehicle Systems, (UVS), and Building Automation Systems (BAS).

SYSTEMS THEORY



Decides

Controller

Influences

Final Control Device

Reacts

The Process

Senses

Measuring Device

- All OT operates on the principles of Systems Theory, and a basic feedback loop

- Control Engineers work to reduce load on the default controller (a human) with a system capable of producing the desired outcome from the physical process under consideration.

Basic Feedback Control Principles | Closed-loop Control Systems | Textbook

Joint Engineer Training
JETC
Conference & Expo

2023
JOINT ENGINEER TRAINING CONFERENCE & EXPO

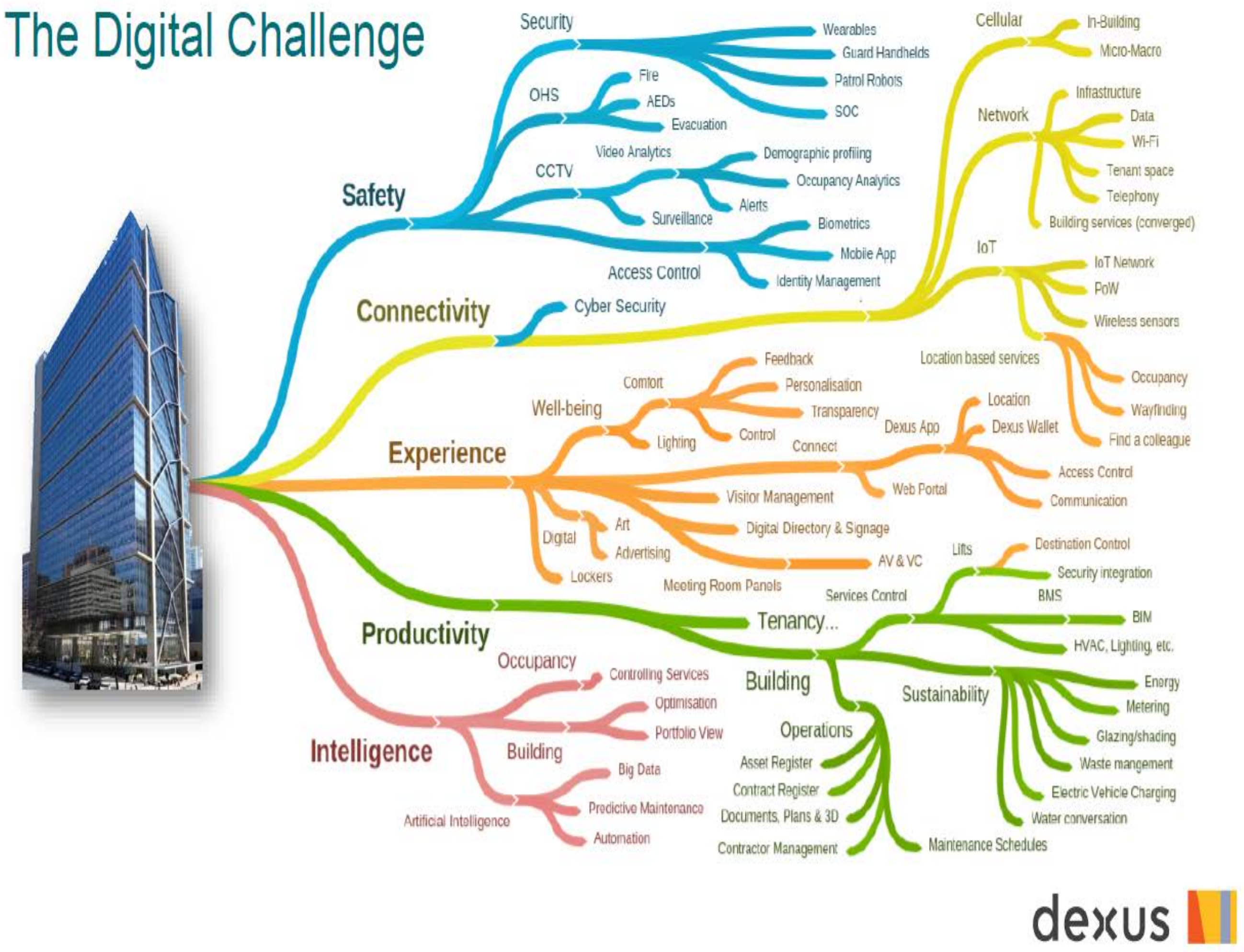
MISSION SUCCESS STARTS HERE
SAMEJETC.ORG

MAY 2-4 2023
San Antonio, TEXAS

SMART TECH FOR BUILDINGS

Industry Trends

- IT and OT networks are Increasingly converged
- More tech being added to drive sustainability and efficiency goals
- Emergence of Installation Resilience Operations Centers (IROC)
- Building systems rely on digital management with both wired and wireless connectivity



OT CYBERSECURITY TRENDS & THREAT ACTORS

INSECURE BY DESIGN

High volume of legacy equipment and insecure protocols require a lower level of sophistication for an attacker to succeed

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

Focus on uptime and vendor restrictions can limit the ability to patch vulnerabilities or install security endpoint tools

HYPERCONNECTIVITY

Leaders want real-time access into operational data, leading to increased interconnectivity

Increased cybersecurity risks with the adoption of Industrial Internet of Things (IIoT) and remote services being used within OT

Industry initiatives including "smart manufacturing", "Industry 4.0", and "digital transformations" are growing in number

INCREASING ATTACKS

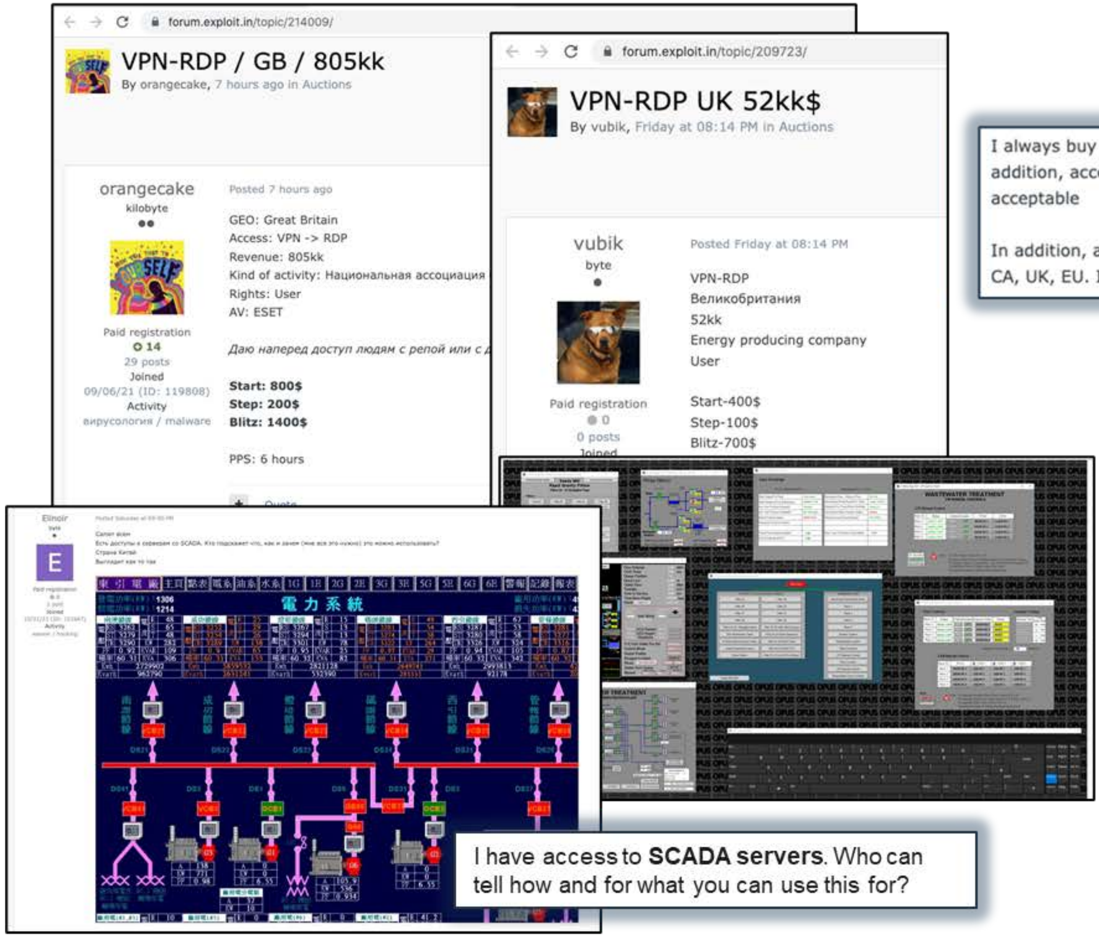
Recent high-profile attacks have increased operational recognition of risks to mission and readiness

700% increase in ransomware within the past two years with heavy focus on post-compromise initiatives targeting critical OT environments

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

WHY OT CYBERSECURITY MATTERS:
ATTACKERS ARE INCREASINGLY TARGETING OT

Growing dark web market for ICS or ‘SCADA access-as-a-service’ and access to other critical infrastructure organizations



forum.exploit.in/topic/214009/

VPN-RDP / GB / 805kk

By orangecake, 7 hours ago in Auctions

orangecake
kilobyte
Paid registration
14
29 posts
Joined
09/06/21 (ID: 119808)
Activity
вирусология / malware

Posted 7 hours ago

GEO: Great Britain
Access: VPN -> RDP
Revenue: 805kk
Kind of activity: Национальная ассоциация
Rights: User
AV: ESET

Даю наперед доступ людям с репой или с д

Start: 800$
Step: 200$
Blitz: 1400$

PPS: 6 hours

forum.exploit.in/topic/209723/

VPN-RDP UK 52kk$

By vubik, Friday at 08:14 PM in Auctions

vubik
byte
Paid registration
0
0 posts
Joined

Posted Friday at 08:14 PM

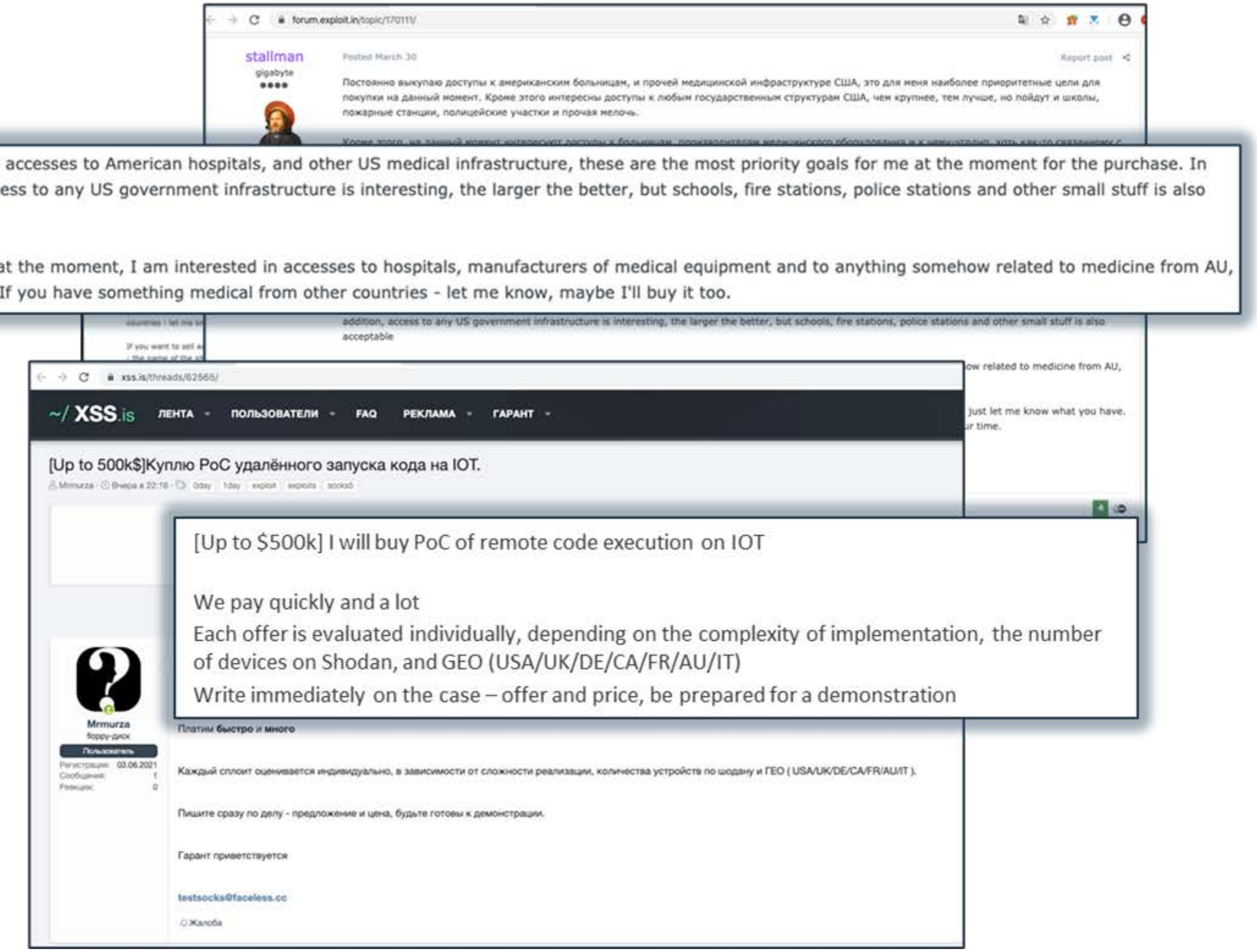
VPN-RDP
Великобритания
52kk
Energy producing company
User

Start-400$
Step-100$
Blitz-700$

Elnoir
byte

Салют всем
Есть доступы к серверам со SCADA. Кто подскажет что, как и зачем (мне все это нужно) это можно использовать?
Страна Китай
Выглядит как то так

I have access to **SCADA servers**. Who can tell how and for what you can use this for?



forum.exploit.in/topic/170111/

stallman
gigabyte

Posted March 30

Report post

Постоянно выкупаю доступы к американским больницам, и прочей медицинской инфраструктуре США, это для меня наиболее приоритетные цели для покупки на данный момент. Кроме этого интересны доступы к любым государственным структурам США, чем крупнее, тем лучше, но пойдут и школы, пожарные станции, полицейские участки и прочая мелочь.

I always buy accesses to American hospitals, and other US medical infrastructure, these are the most priority goals for me at the moment for the purchase. In addition, access to any US government infrastructure is interesting, the larger the better, but schools, fire stations, police stations and other small stuff is also acceptable

In addition, at the moment, I am interested in accesses to hospitals, manufacturers of medical equipment and to anything somehow related to medicine from AU, CA, UK, EU. If you have something medical from other countries - let me know, maybe I'll buy it too.

xss.is/threads/62565/

[Up to 500k$]Куплю PoC удалённого запуска кода на IOT.

Mrmurza · Вчера в 22:16 · 0day 1day exploit exploits socks5

[Up to $500k] I will buy PoC of remote code execution on IOT

We pay quickly and a lot

Each offer is evaluated individually, depending on the complexity of implementation, the number of devices on Shodan, and GEO (USA/UK/DE/CA/FR/AU/IT)

Write immediately on the case – offer and price, be prepared for a demonstration

Mrmurza
floppy-диск
Пользователь
Регистрация: 03.06.2021
Сообщения: 1
Реакции: 0

Платим **быстро** и **много**

Каждый сплоит оценивается индивидуально, в зависимости от сложности реализации, количества устройств по шодану и ГЕО (USA/UK/DE/CA/FR/AU/IT).

Пишите сразу по делу - предложение и цена, будьте готовы к демонстрации.

Гарант приветствуется

testsocks@faceless.cc

Жалоба

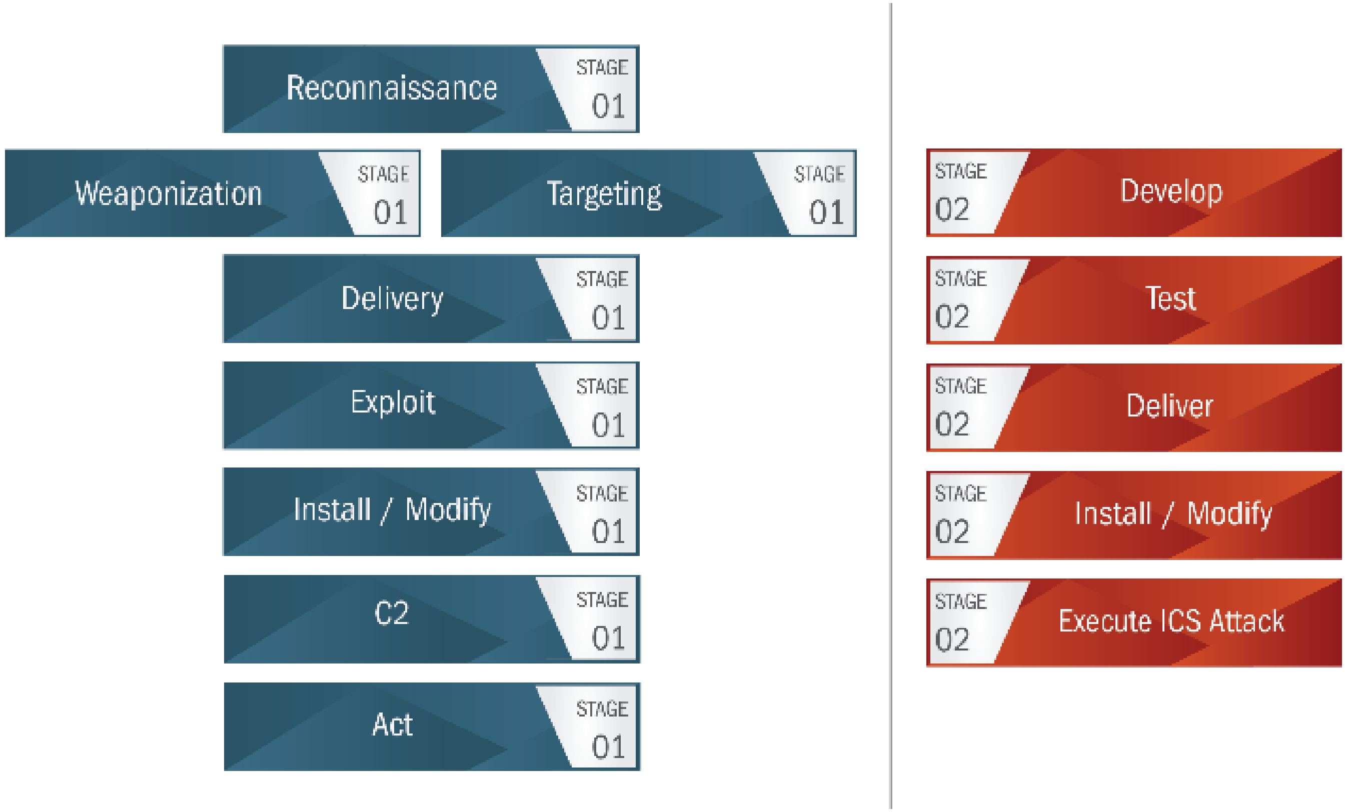
INDUSTRIAL CONTROL SYSTEM KILL CHAIN

- **ICS Attacks occur in two stages:**
  1. **Cyber Intrusion Preparation & Execution**
  2. **ICS Attack Development & Execution**

- **The amount of reconnaissance and preparation is directly proportional to the potential for a destructive impact**

- **All destructive ICS/OT cyber attacks require pre-reconnaissance of the victim network**

- **The need for pre-reconnaissance gives defenders an advantage**



USA TODAY™

- October, 12, 2021

”The next big cyberthreat isn't ransomware. It's killware. And it's just as bad as it sounds.”

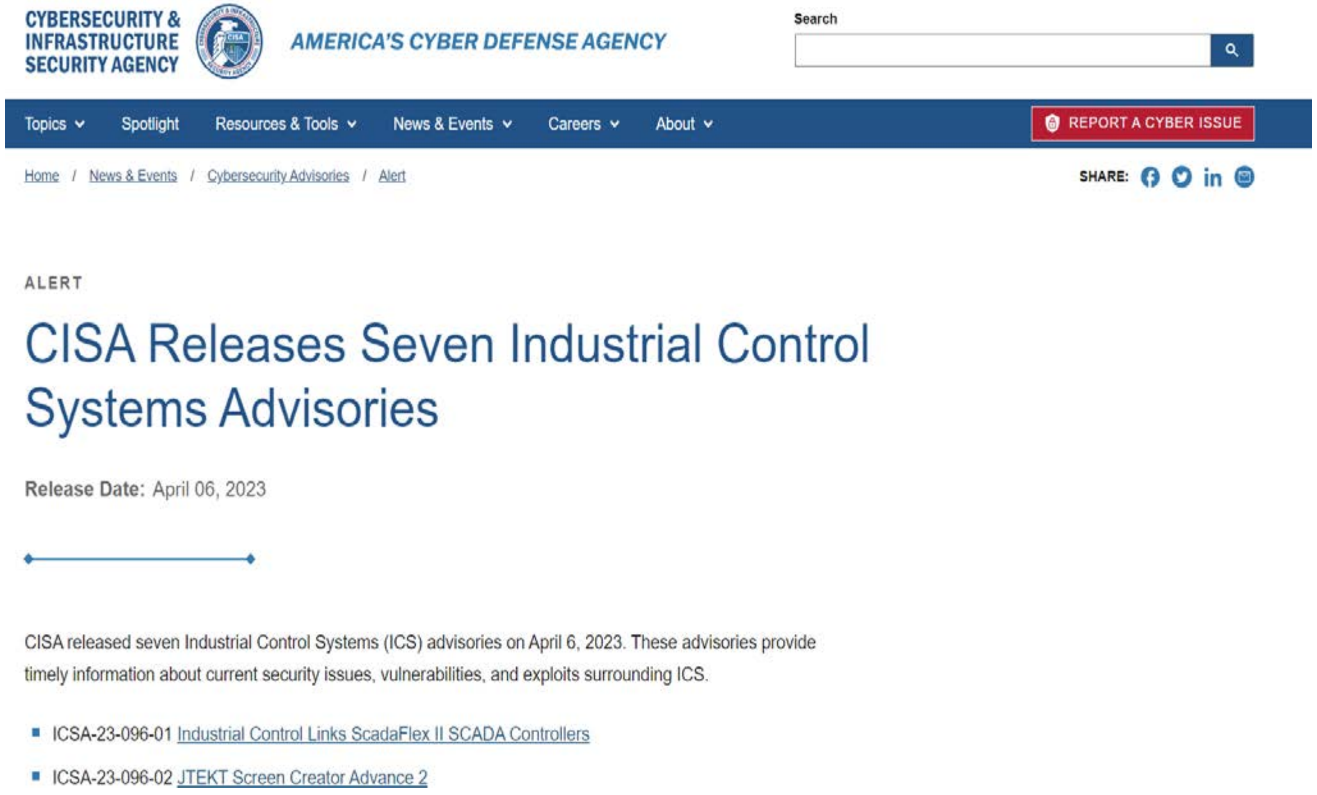
The nation’s top homeland security official is worried about an even more dire digital danger: killware, or cyberattacks that can literally end lives.

- “The hack of a water treatment facility in February 2021 demonstrated the grave risks that malicious cyber activity poses to public health and safety. The attacks are increasing in frequency and gravity, and cybersecurity must be a priority for all of us.”
- “Soon, CEOs won’t be able to plead ignorance or retreat behind insurance policies.”

THE U.S. GOVERNMENT RESPONSE

- **March 2022 - President Biden's Statement on our Nation's Cybersecurity**
  - "This is a critical moment to accelerate our work to improve domestic cybersecurity and bolster our national resilience."
  - "Potential that Russia could conduct malicious cyber activity against the United States, including as a response to the unprecedented economic costs we've imposed on Russia
  - "Evolving intelligence that the Russian Government is exploring options for potential cyberattacks.
- **March 2022 – US Security & Exchange Commision (SEC) Proposes New Cybersecurity Disclosure Rules on Incident Reporting, Risk Management, Strategy, and Governance**
  - "SEC determined that investors would benefit from "more timely and consistent disclosures" by public companies of several categories of cybersecurity-related information: (1) material cybersecurity incidents, (2) risk management and strategy, (3) governance, and (4) cybersecurity expertise among board members."
  - New rule require disclosure whether (1) the company has a cybersecurity risk assessment and management program (if so, the rule would require a description); (2) the company engages third parties in connection with the program; and (3) the company has policies and procedures in place to evaluate cyber risks associated with third-party service providers.
- **February 2022 DHS Cyber Security and Infrastructure Agency (CISA) – "Shields Up" Program**
  - "All organizations—regardless of size—adopt a heightened protection posture when it comes to cybersecurity and protecting their most critical assets."

CYBER SECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA)


CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
AMERICA'S CYBER DEFENSE AGENCY
Search
Topics
Spotlight
Resources & Tools
News & Events
Careers
About
REPORT A CYBER ISSUE
Home / News & Events / Cybersecurity Advisories / Alert
SHARE:

ALERT

CISA Releases Seven Industrial Control Systems Advisories

Release Date: April 06, 2023

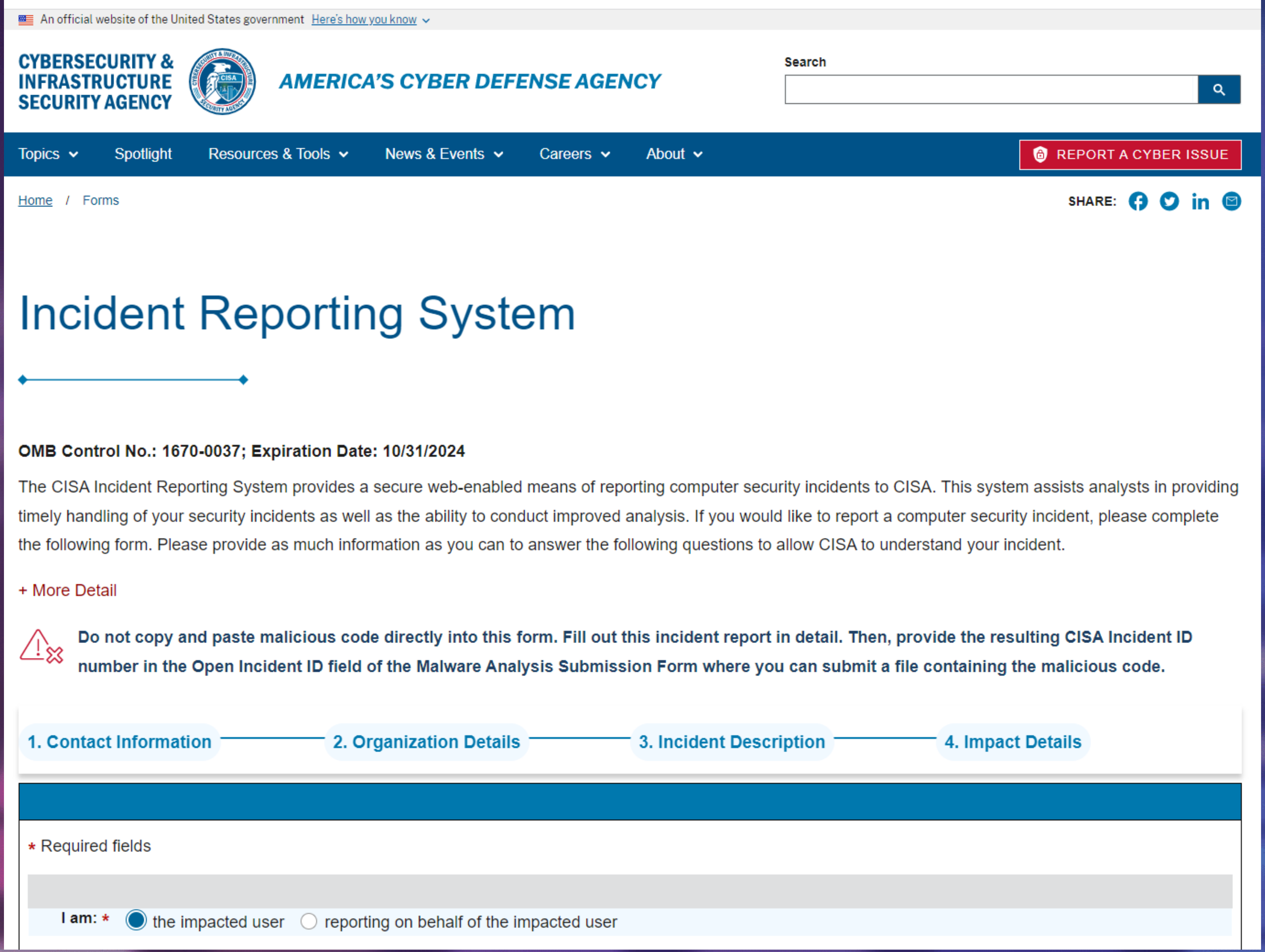
CISA released seven Industrial Control Systems (ICS) advisories on April 6, 2023. These advisories provide timely information about current security issues, vulnerabilities, and exploits surrounding ICS.

- ICSA-23-096-01 Industrial Control Links ScadaFlex II SCADA Controllers
- ICSA-23-096-02 JTEKT Screen Creator Advance 2

DHS CISA: https://www.cisa.gov/topics/industrial-control-systems https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf
DHS CISA: https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf

- CISA maintains database of all types of cyber attacks to inform Command Authorities on trends and emerging threats

- Mandatory Reporting Requirement for Federal Agencies



An official website of the United States government Here's how you know
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
AMERICA'S CYBER DEFENSE AGENCY
Search
Topics
Spotlight
Resources & Tools
News & Events
Careers
About
REPORT A CYBER ISSUE
Home / Forms
SHARE:

Incident Reporting System

OMB Control No.: 1670-0037; Expiration Date: 10/31/2024

The CISA Incident Reporting System provides a secure web-enabled means of reporting computer security incidents to CISA. This system assists analysts in providing timely handling of your security incidents as well as the ability to conduct improved analysis. If you would like to report a computer security incident, please complete the following form. Please provide as much information as you can to answer the following questions to allow CISA to understand your incident.

+ More Detail

Do not copy and paste malicious code directly into this form. Fill out this incident report in detail. Then, provide the resulting CISA Incident ID number in the Open Incident ID field of the Malware Analysis Submission Form where you can submit a file containing the malicious code.

1. Contact Information — 2. Organization Details — 3. Incident Description — 4. Impact Details

* Required fields

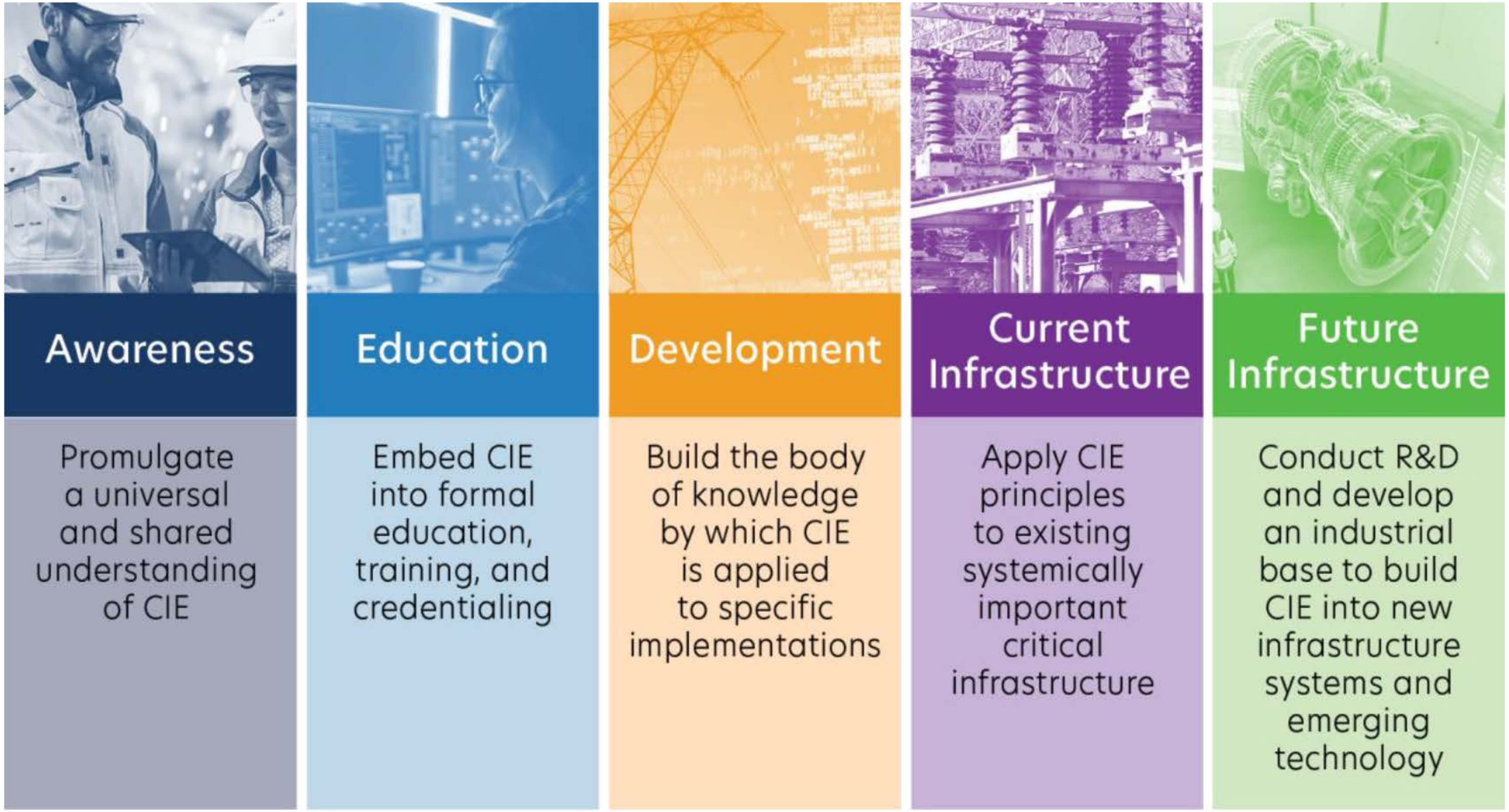
I am: * ● the impacted user ○ reporting on behalf of the impacted user

THE U.S. NATIONAL CYBER STRATEGY

- **Released on March 1, 2023 to replace 2018 Strategy**
  - “Cybersecurity is essential to the basic functioning of our economy, the operation of our critical infrastructure, the strength of our democracy and democratic institutions, the privacy of our data and communication, and our national defense.”
  - “The Strategy recognizes that government must use all tools of national power in a coordinated manner to protect our national security, public safety, and economic prosperity,”
- **Seeks to build and enhance collaboration around five pillars:**
  - Defend Critical Infrastructure and Operational Technologies
  - Disrupt and Dismantle Threat Actors;
  - Shape Market Forces to Drive Security and Resilience;
  - Invest in a Resilient Future through strategic investments and coordinated, collaborative action to lead the world in the innovation of secure and resilient next-generation technologies and infrastructure;
  - Forge International Partnerships to Pursue Shared Goals.
- **Promotes increased collaboration with the Private Sector**

NATIONAL CYBER-INFORMED ENGINEERING (CIE) STRATEGY

- Published by the Department of Energy in June 2022
- Currently developing an Implementation Plan
- While written for the energy sector – applies to all critical infrastructure



Awareness

Promulgate a universal and shared understanding of CIE

Education

Embed CIE into formal education, training, and credentialing

Development

Build the body of knowledge by which CIE is applied to specific implementations

Current Infrastructure

Apply CIE principles to existing systemically important critical infrastructure

Future Infrastructure

Conduct R&D and develop an industrial base to build CIE into new infrastructure systems and emerging technology

CONGRESSIONAL DIRECTION

NDAA - National Defense Authorization Act

- **Sec 1650 of FY 2017 NDAA** required evaluations of cyber vulnerabilities of DOD critical infrastructure, including new, innovative methodologies or engineering approaches to:
  1. Improve the defense of control systems against cyber attacks;
  2. Increase the resilience of military installations against cybersecurity threats;
  3. Prevent or mitigate the potential for high-consequence cyber attacks; and
  4. Inform future requirements for the development of such control systems.
- **Sec 1639 of FY2018 NDAA** directed CS/OT be included in the Cyber Scorecard to the Secretary of Defense
- **Sec 1643 of FY2019 NDAA** directed SECDEF to designate one official to be responsible for matters relating to integrating cybersecurity and industrial control systems for DoD.

CONGRESSIONAL DIRECTION

NDAA - National Defense Authorization Act

- **Sec 1505 of the FY 2022 NDAA** directs SECDEF, the Commander of USCYBERCOM, and the military services to complete the mapping of the "mission relevant terrain" for Defense Critical Assets so they can be defended from a cybersecurity threat and to:

1. Create and implement baseline cyber requirements for CS/OT across the DoD;
2. Achieve visibility of CS/OT within all of DoD's "forces, facilities, installations and bases, critical infrastructure, and weapon systems;" and
3. Establish C2 over and be able to defend CS/OT systems, including implementing concept of operations for defense of CS/OT, sensoring OT networks, and establishing processes for incident reporting, compliance, and vulnerability management; and
4. Make "necessary investments" to secure CS/OT and to establish dedicated funding for remediation of cybersecurity gaps in CS/OT.

https://www.nightdragon.com/insights/dod-must-secure-its-control-systems-there-is-no-pass-fail/

CYBERSECURITY STANDARDS FOR ICS AND OTHER OT

<u>Federal standards under NIST and Industry Standards under ISA provide guidance</u>

- National Institute of Standards and Technology - NIST SP 800-82 Revision 2 *Guide to Industrial Control Systems (ICS) Security*
  - http://dx.doi.org/10.6028/NIST.SP.800-82r2

  Provides guidance which is compulsory under FIPS 199 and 200 for agencies and departments of the executive branch

- International Society of Automation - ISA/IEC 62443 Series – Cybersecurity of Industrial Automated Control Systems
  - https://www.isa.org/standards/

  The ISA Standards serve as an the de facto internationally recognized standard for cyber security of Operational Technologies. Adapted for facilities by BuildingCyberSecurity.org

FEDERAL GUIDANCE

- **UFC 4-010-06**,Cybersecurity of Facility-Related Control Systems, With Change 1 and any other change pending
- **UFGS 25 08 10**, Utility Monitoring And Control System Testing
- **UFGS 25 10 10**, Utility Monitoring and Control System (UMCS) Front End And Integration
- **UFGS 25 05 11**, Cybersecurity For Facility-Related Control Systems
- Control Systems Cyber Defense Reference Architecture (CSCDRA), March 03, 2022
- Federal/DOD Guidance on the Implementation of Zero Trust Architecture (ZTA) (NIST, Cybercom, CIA):

DOD/SERVICE GUIDANCE

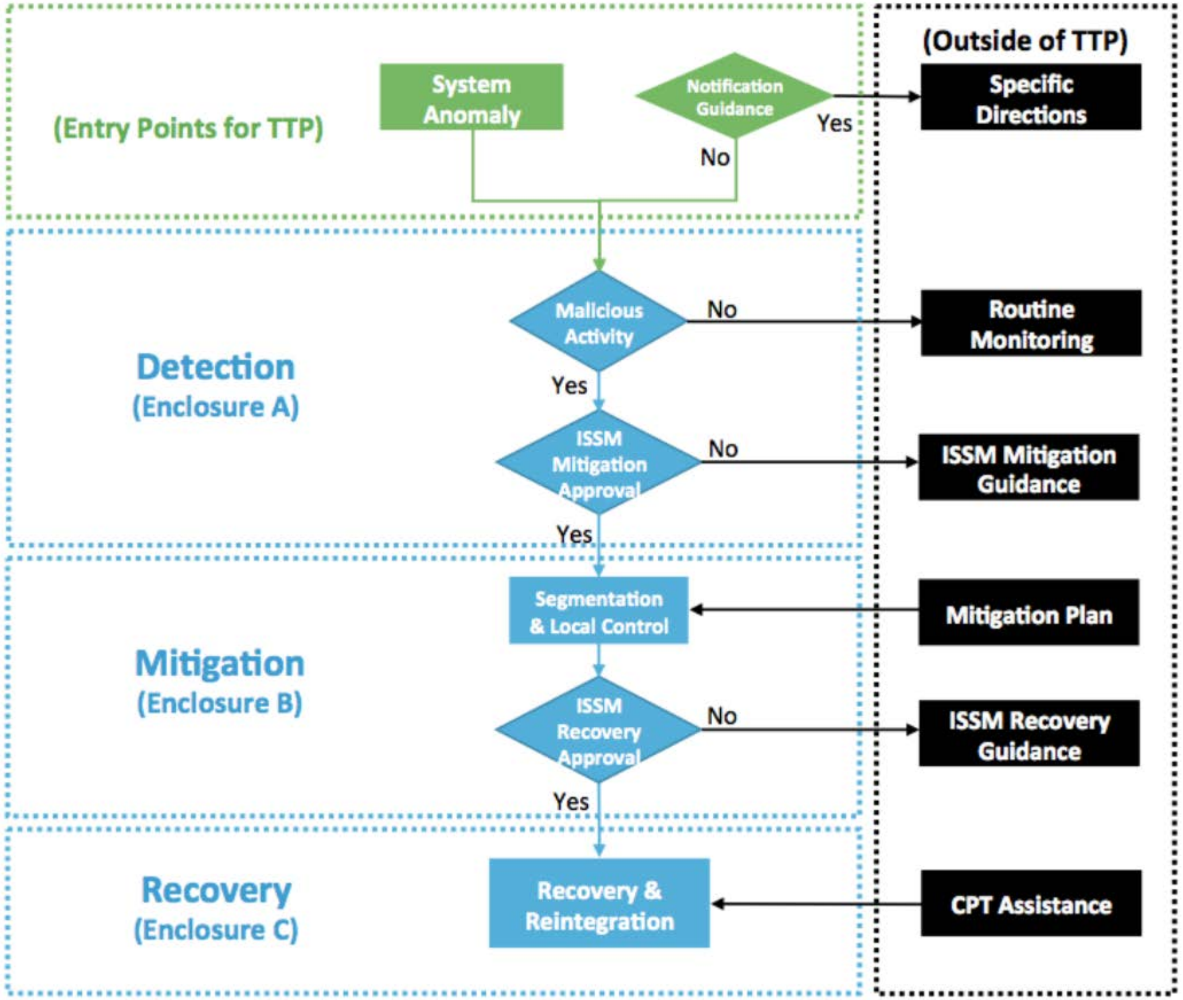
- Control Systems Cyber Defense Reference Architecture (CSCDRA), March 03, 2022
- DOD CONTROL SYSTEMS SECURITY REQUIREMENTS GUIDE Version 1, Release 1 January 26, 2021
- **Advanced Cyber Industrial Control System Tactics, Techniques, and Procedures (ACI TTP) for Department of Defense (DOD) Industrial Control Systems (ICS)**
- The Department of Defense Cyber Table-Top Guide Version 2.0 16 September 2021
- Authorities To Operate (only those related to OT)
- Control System Cyber Defense Reference Architecture (More Situational Awareness Or Industrial Control Systems , MOSAICS)
- DAFGM2021-32-01 Department of the Air Force Guidance Memorandum, Civil Engineer Control Systems Cybersecurity, January 05, 2021

ADVANCED CYBER INDUSTRIAL CONTROL SYSTEM TACTICS, TECHNIQUES, AND PROCEDURES (ACI TTP) FOR DEPARTMENT OF DEFENSE (DOD) INDUSTRIAL CONTROL SYSTEMS (ICS)

This ACI TTP is divided into sections:

1. **ACI TTP Concepts (chapters 2 through 4)**

2. **Threat-Response Procedures (Detection, Mitigation, Recovery) (enclosures A, B, and C)**



Joint Engineer Training Conference & Expo
JETC

2023
JOINT ENGINEER TRAINING CONFERENCE & EXPO

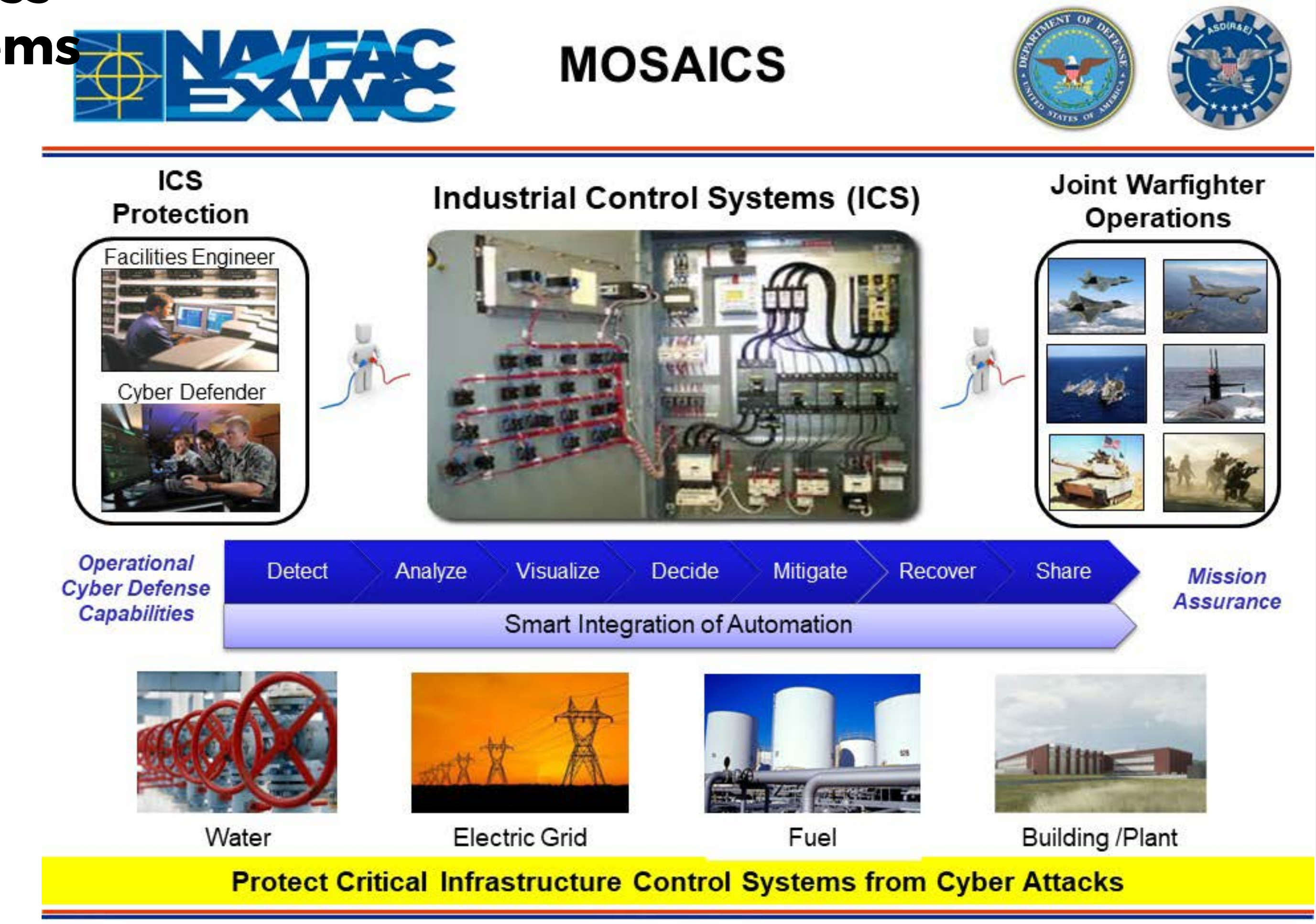
MISSION SUCCESS STARTS HERE
SAMEJETC.ORG

MAY 2-4 2023
San Antonio, TEXAS

MOSAICS

More Situational Awareness For Industrial Control Systems

- First-ever comprehensive, integrated and automated solution for industrial control systems cybersecurity.
- Capability to "detect, mitigate and recover from a cyber attack on Industrial Control Systems (ICS) networks combined with decision support, analytics, visualization, and information sharing tools."



NAVFAC EXWC MOSAICS

ICS Protection
Facilities Engineer
Cyber Defender

Industrial Control Systems (ICS)

Joint Warfighter Operations

Operational Cyber Defense Capabilities

Detect → Analyze → Visualize → Decide → Mitigate → Recover → Share

Smart Integration of Automation

Mission Assurance

Water
Electric Grid
Fuel
Building /Plant

Protect Critical Infrastructure Control Systems from Cyber Attacks

COMMON ATTACK VECTORS

- Phishing emails are the most common way to gain a first foothold
- Vendor maintenance laptops
- Remote maintenance connections
- Drones and other physical intrusions can create nodes in a wireless network otherwise out of reach for attackers
- Rogue USB devices, while not as prevalent as they used to be, are still a threat

A WIDE THREAT AND PAYLOAD DELIVERY FOR CYBER ATTACKS

1. Malware – malicious software - program or code that is created to do harm to a computer, network or server.
2. Denial-of-Service (DoS) Attacks – Flood a network with false requests in order to disrupt business operations
3. Phishing – Using email, SMS, phone, social media, to entice a victim to share sensitive information
4. Ransomware – the victim's system is digitally seized and held hostage until a ransom is paid to the attacker.
5. Zero Day – Exploiting a design flaw in the security of software or firmware to attack a network
6. Spoofing – Cybercriminal disguises themselves as a known or trusted source.
7. Identity-Based Attacks – Compromising and using a valid user's credentials to masquerade as that user
8. Code Injection Attacks – Injecting malicious code into a vulnerable computer/network to change its action.
9. Supply Chain Attacks – Targets a trusted third-party vendor who offers services or software.
10. Insider Threats – Current or former employees with direct access to networks or sensitive data
11. More? – Threat vectors and innovation are growing every day.

CYBER INDUSTRY GOV'T ENGAGEMENT (IGE)

"First time in SAME history connecting IGE with a warfighting seminar to highlight critical mission imperatives"

Initiated by SAME in October 2021 with a Distinct 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**

WARFIGHTING SEMINAR LEARNING OBJECTIVES

- ✓ Review processes to **identify** critical systems and cyber vulnerabilities within a risk management framework;
- ✓ Identify proactive measures to **protect** critical systems and mitigate risk of a cyber physical attack;
- ✓ Present methods to **detect** and confirm the origin and method of a cyber attack and damage assessment;
- ✓ Develop checklists and protocols to quickly isolate, **respond** and communicate progress to the incident;
- ✓ Assess options, probabilities and timing for the **recovery** of mission essential system;
- ✓ Identify programs to **share information** within the National Security command structure on the incident

AGENDA

Wednesday, May 3, 2023

10:30 am - 1:00 pm – Scenario Training - Mission Recovery from a Cyber Physical System (CPS) Attack to a Domestic National Security Asset

- Open to all JETC Participants to observe, ask questions, engage in discussion
- Team will walk through an actual attack scenario and review courses of action
- Participants will receive information to enhance protections and incident response
- Breaks will be determined by facilitators based on pace of presentation

1 pm - 2:00 pm - Panel/Audience Feedback and Out-Brief Prep

2:30 pm - 5:00 pm - Large Group Out-Brief to Senior Leaders

- (findings, possible paths forward, and follow on actions)

END OF INTRODUCTION

OT CYBER SEMINAR

OPENING REMARKS

AUDIENCE PARTICIPATION

This is not a Red v Blue (yet) exercise, but an educational seminar

- This is a learning and awareness opportunity - discussion definitely encouraged at any point
- Chatham House Rule for discussion - Neither the identity nor the affiliation of the speaker, nor that of any other participant, may be revealed.
- Moderators will recognize hands up and reserve the right to park discussion and keep us on topic
- When raising issues or questions, please keep them succinct and relevant to the topic
- Please participate in the polls
- This is the first time for the Team presenting an OT scenario - Please offer feedback to make the training more effective

AUDIENCE PARTICIPATION

What each audience member should be wondering

- □ What are the risks to my mission?
- □ Is my organization prepared?
- □ What can I take away for my unit or company?
- □ Who else should receive this presentation?
- □ How collectively do we reduce this threat?

SCENARIO

THE TARGET

- Building 1 is a large, recently constructed multi-story Unified Command headquarters facility supporting critical National Security Missions
- Building 1 is on a Joint Base, in a Midwest State managed by the Air Force.
- Building 1 contains a Joint Operations Center (JOC), multiple levels of data security and SCIFS, and high value personnel
- Building 1 is a security compartmentalized facility requiring badged entry
- The data and IT missions in Bldg 1's SCIFS and JOC require consistent cooling

BUILDING 1 - OPERATIONAL TECHNOLOGIES

- Fire Systems
  - Fire Detection Systems (alarms)
  - Fire Suppression Systems
- HVAC Systems
  - Ventilation, Chillers, Air Handling, Purification
  - Air Quality, Health
- Vertical Transport Systems
  - Elevators
  - Escalators
- Lighting Systems
  - Standard lighting and shades
  - Emergency lighting
- Utility Components & Systems
  - Gas
  - Water, Boilers, Filtration
  - Power supply (including Backup Generators, UPS)
- Building Automation Systems (BAS)
- Electronic Security System (ESS)
  - Physical Security Control
  - Physical Access
  - Video Surveillance
- Mass Notification Systems
  - Standard
  - Emergency
  - Digital Signage
- Voice Communication Systems
  - Standard, Emergency
  - Wired and wireless
- Parking Systems
  - Access
  - EV Charging
- Information Technologies
  - Owner Network
  - Property Management

AUDIENCE QUESTIONS

- Which one of these systems, if compromised, could threaten human life?

- Which systems could threaten equipment in the building?

- Which systems could compromise mission security? Broader impact to mission?

We'll give you a few minutes...

KEY PERSONNEL

Joint Base Team

Base Civil Engineering/ Public Works

- Facility trades/technicians comprised of civilian and military personnel
- Installation Engineering staffs comprised of discipline engineers
- Contract Management for facility system warranties
- The Base Civil Engineer

Mission Support Group

- Communication Squadron managing installation data networks and IT systems
- Contracting Officer
- Security Police
- Public Affairs
- Legal Counsel
- Base Chaplain

Building 1

- Facilities Team
- Building Data Network management staff
- Joint Op Center
- HQ Staff
- 4-Star CC
- Public Affairs
- COOP Team
- US CYBERCOM Rep

AIR CONDITIONING GOES OUT IN GENERAL'S OFFICE…

- HVAC Technician discovers burnt out blower motor and faulted VFD.
- Technician replaces motor and VFD from BCE stock.
- Technician programs new VFD from running project on HVAC System PLCs.

TEMPS RISING THROUGHOUT BLDG 1

- Heating, Ventilation, and Air Conditioning (HVAC) systems go offline
- The office areas and JOC ambient temperatures are rising noticably

HVAC Technicians respond to troubleshoot

HVAC System

Building Automation System HMI

TROUBLESHOOT HVAC

- VFDs are no longer functioning building wide
- VAVs are going offline
- Blower motors are burning out throughout the building HVAC plant

First Remedy

- Swap out with new motors from BCE stock
- Swap out VFDs and reprogram from from BAS Engineering Workstation
- Check PLC settings and logs
- Escalate to Installation & Alert Ops

THE OUTAGE HAS SPREAD TO THE ENTIRE BUILDING

Shortly after startup, all HVAC motors burn out resulting in building wide outage.

Check Power Supply

and Confirm with Electrical Shop for power surges

POWER CHECK

Main Power is Clean

Nothing is Tripped

Check Programable Logic Controllers (PLCs)

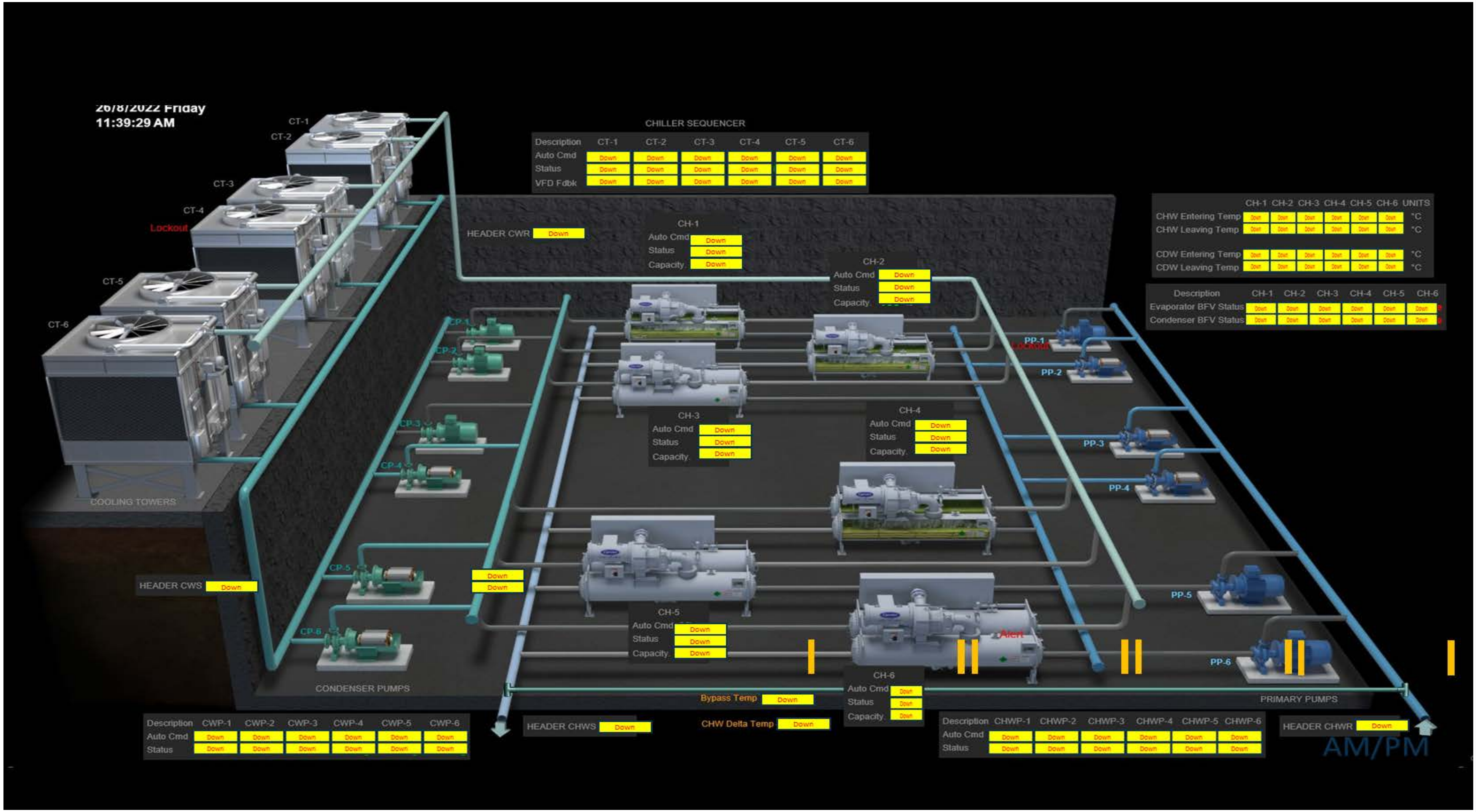
Troubleshoot Building Automation System (BAS)

Joint Engineer Training
JETC
Conference & Expo

2023
JOINT ENGINEER TRAINING CONFERENCE & EXPO

MISSION SUCCESS STARTS HERE
SAMEJETC.ORG

MAY 2-4 2023
San Antonio, TEXAS



26/8/2022 Friday
11:39:29 AM

CHILLER SEQUENCER

Description	CT-1	CT-2	CT-3	CT-4	CT-5	CT-6
Auto Cmd	Down	Down	Down	Down	Down	Down
Status	Down	Down	Down	Down	Down	Down
VFD Fdbk	Down	Down	Down	Down	Down	Down

	CH-1	CH-2	CH-3	CH-4	CH-5	CH-6	UNITS
CHW Entering Temp	Down	Down	Down	Down	Down	Down	°C
CHW Leaving Temp	Down	Down	Down	Down	Down	Down	°C
CDW Entering Temp	Down	Down	Down	Down	Down	Down	°C
CDW Leaving Temp	Down	Down	Down	Down	Down	Down	°C

Description	CH-1	CH-2	CH-3	CH-4	CH-5	CH-6
Evaporator BFV Status	Down	Down	Down	Down	Down	Down
Condenser BFV Status	Down	Down	Down	Down	Down	Down

HEADER CWR Down

CH-1
Auto Cmd Down
Status Down
Capacity Down

CH-2
Auto Cmd Down
Status Down
Capacity Down

CH-3
Auto Cmd Down
Status Down
Capacity Down

CH-4
Auto Cmd Down
Status Down
Capacity Down

CH-5
Auto Cmd Down
Status Down
Capacity Down

CH-6
Auto Cmd Down
Status Down
Capacity Down

HEADER CWS Down

Down
Down

Bypass Temp Down

CHW Delta Temp Down

HEADER CHWS Down

HEADER CHWR Down

Description	CWP-1	CWP-2	CWP-3	CWP-4	CWP-5	CWP-6
Auto Cmd	Down	Down	Down	Down	Down	Down
Status	Down	Down	Down	Down	Down	Down

Description	CHWP-1	CHWP-2	CHWP-3	CHWP-4	CHWP-5	CHWP-6
Auto Cmd	Down	Down	Down	Down	Down	Down
Status	Down	Down	Down	Down	Down	Down

Joint Engineer Training
JETC
Conference & Expo

2023
JOINT ENGINEER TRAINING CONFERENCE & EXPO

MISSION SUCCESS STARTS HERE
SAMEJETC.ORG

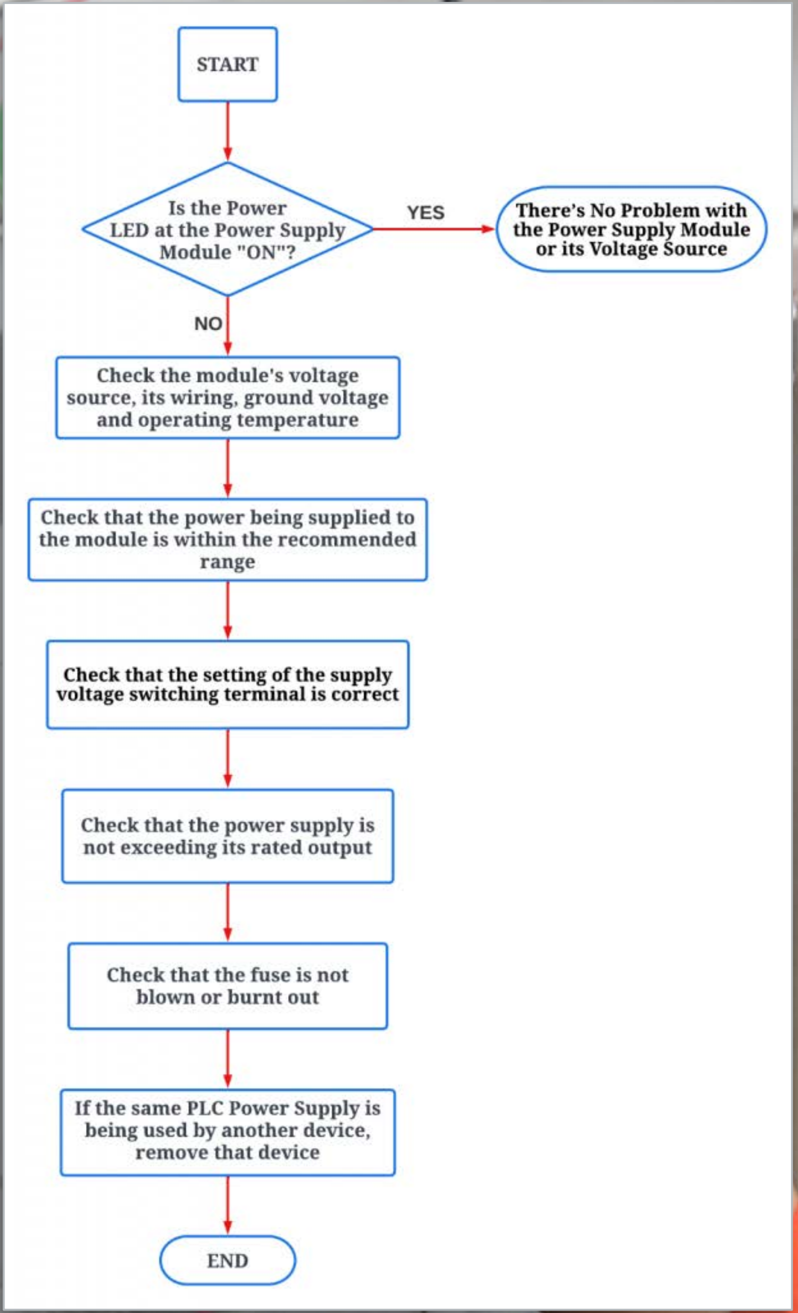
MAY 2-4 2023
San Antonio, TEXAS

TROUBLESHOOT PLCs

- **First, Check PLC Performance**

- **Second, Check the PLC logs for data anomalies**
  - PLC display shows new project downloaded at 03:00.
  - New program drives VFDs into a destructive state at or after 09:00
  - The project change wasn't authorized through change management

This is indicative of an attack



START

Is the Power LED at the Power Supply Module "ON"?

YES

There's No Problem with the Power Supply Module or its Voltage Source

NO

Check the module's voltage source, its wiring, ground voltage and operating temperature

Check that the power being supplied to the module is within the recommended range

Check that the setting of the supply voltage switching terminal is correct

Check that the power supply is not exceeding its rated output

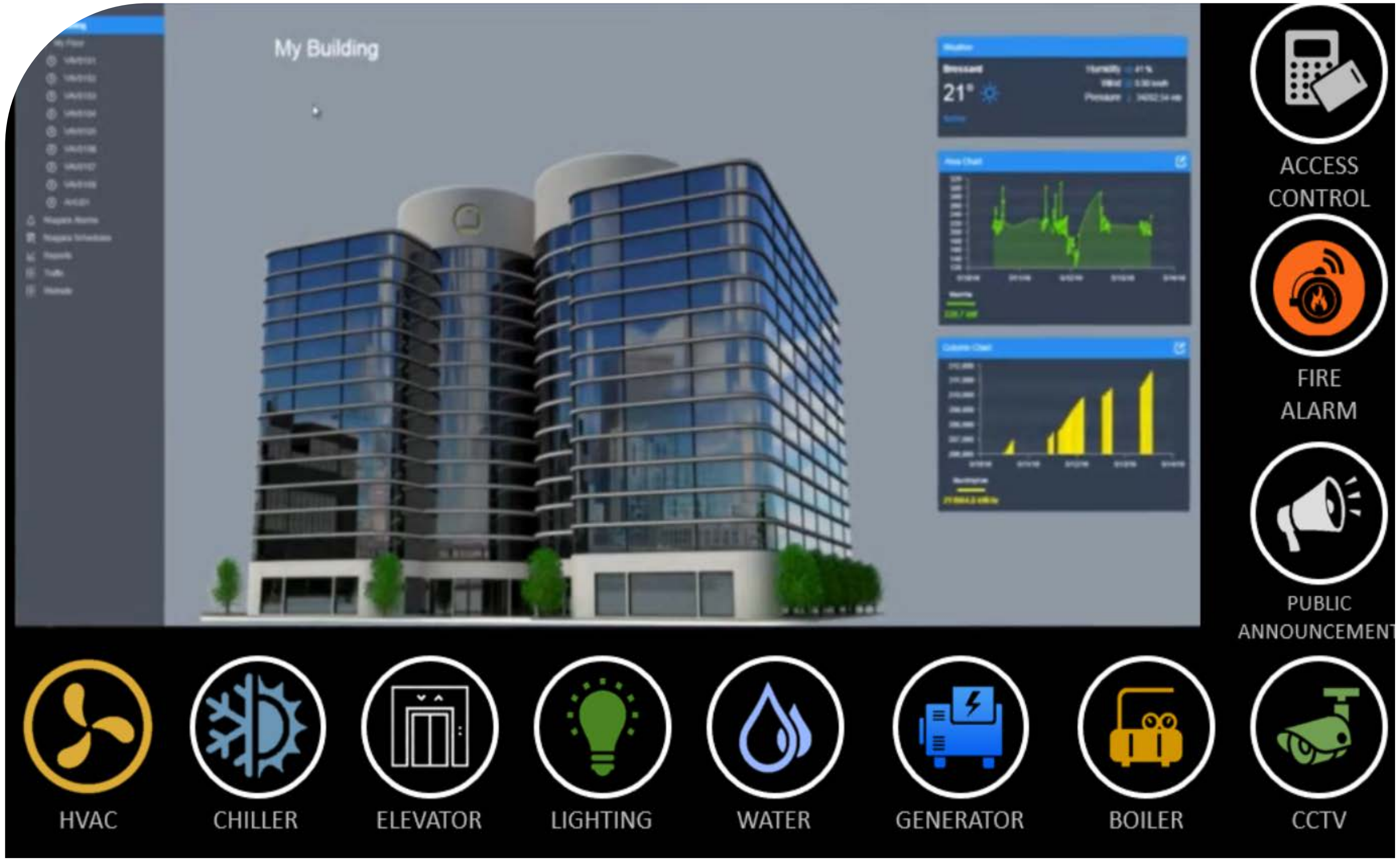
Check that the fuse is not blown or burnt out

If the same PLC Power Supply is being used by another device, remove that device

END

TROUBLESHOOT BAS

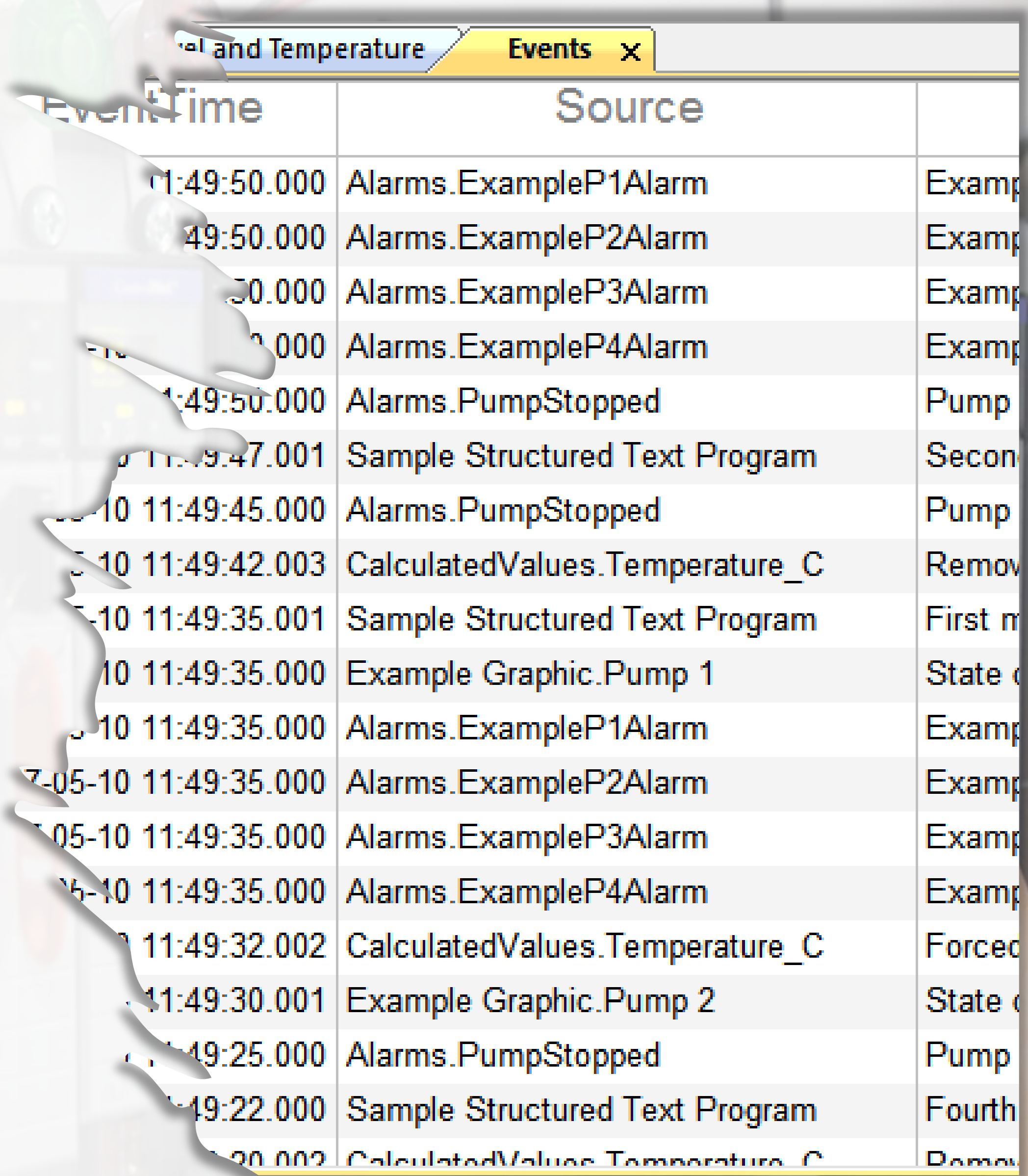
- BAS HMI is reporting normal operation and normal room temperatures –
- No change in reported ambient temperature from before HVAC outage
- **Incorrect timestamps, defacement, false and inconsistent sensor and system data, and set-points manipulated without authorization are all possible indicators of a compromise**



FURTHER ANALYSIS OF BAS

Check BAS Data for recent activity

- Building Automation System Data Historian log shows a remote admin login from Engineering workstation at 01:30, then a series of entries with yesterday's date on the timestamps from that logon until now.



EventTime	Source	
1:49:50.000	Alarms.ExampleP1Alarm	Examp
49:50.000	Alarms.ExampleP2Alarm	Examp
0.000	Alarms.ExampleP3Alarm	Examp
.000	Alarms.ExampleP4Alarm	Examp
:49:50.000	Alarms.PumpStopped	Pump
.47.001	Sample Structured Text Program	Secon
10 11:49:45.000	Alarms.PumpStopped	Pump
10 11:49:42.003	CalculatedValues.Temperature_C	Remov
-10 11:49:35.001	Sample Structured Text Program	First m
10 11:49:35.000	Example Graphic.Pump 1	State c
10 11:49:35.000	Alarms.ExampleP1Alarm	Examp
7-05-10 11:49:35.000	Alarms.ExampleP2Alarm	Examp
05-10 11:49:35.000	Alarms.ExampleP3Alarm	Examp
5-10 11:49:35.000	Alarms.ExampleP4Alarm	Examp
11:49:32.002	CalculatedValues.Temperature_C	Forced
11:49:30.001	Example Graphic.Pump 2	State c
49:25.000	Alarms.PumpStopped	Pump
49:22.000	Sample Structured Text Program	Fourth
20.002	CalculatedValues.Temperature_C	Remov

This is another indication of an attack

CONTACT CONTROL SYSTEMS VENDORS AND MANUFACTURERS

- **Explain incident**
- **Have system model numbers and installation dates ready**
- **Provide warranty account number…**
- **Remote login to the system?** (Note: This violates UFC)
  - Is it secure?
  - If you log them in, the infection may spread
- **Determine Operating System and confirm last firmware version and/or patch update**
- **Determine existence of similar incidents**
- **Some OEMs vendors have Cyber Security Service Providers to assist**

AUDIENCE QUESTION

- Are you confident that your facility engineers have a written inventory of all building systems information needed to make this call?

- Is that information accessible in more than one format?

FIRST OBSERVATION

1. Significant HVAC System catastrophic Failure in Bldg 1
2. No known cause of mechanical failure
3. Evidence of System data, software or firmware manipulation
4. No Short Term Fix
5. No estimate time of restoration

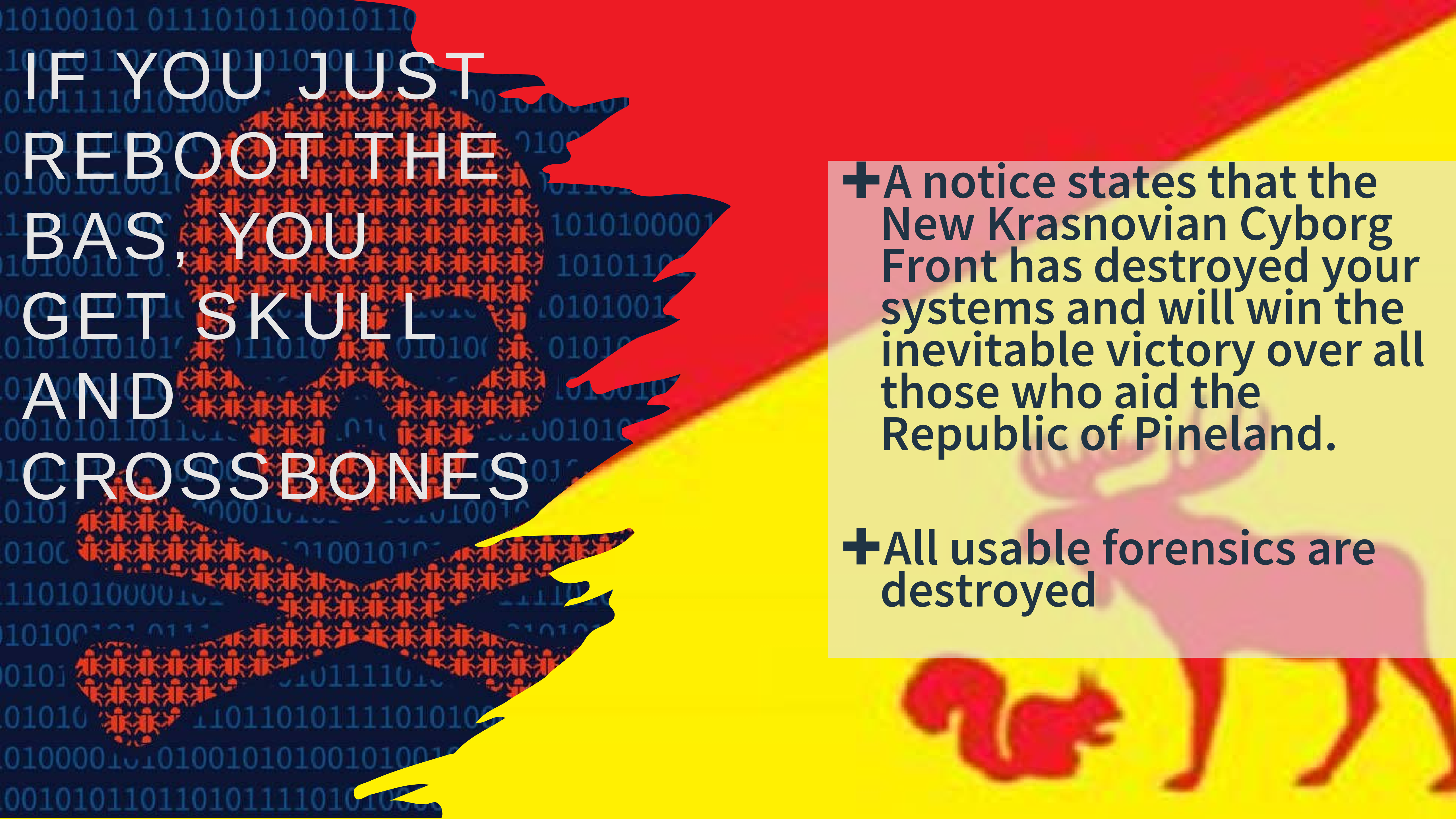
Need Comm Squadron expertise to check networks, data, and access management logs

ADDITIONAL PRESSURE

- The New Krasnovian Cyborg Front have released a video to the press, claiming a major cyber victory and vowing more action until the U.S. stops propping up the evil Republic of Pineland. Many news outlets are running it at 5:00
- Calls start coming in from various media outlets

- **The actor may or may not take credit**

IF YOU JUST REBOOT THE BAS, YOU GET SKULL AND CROSSBONES

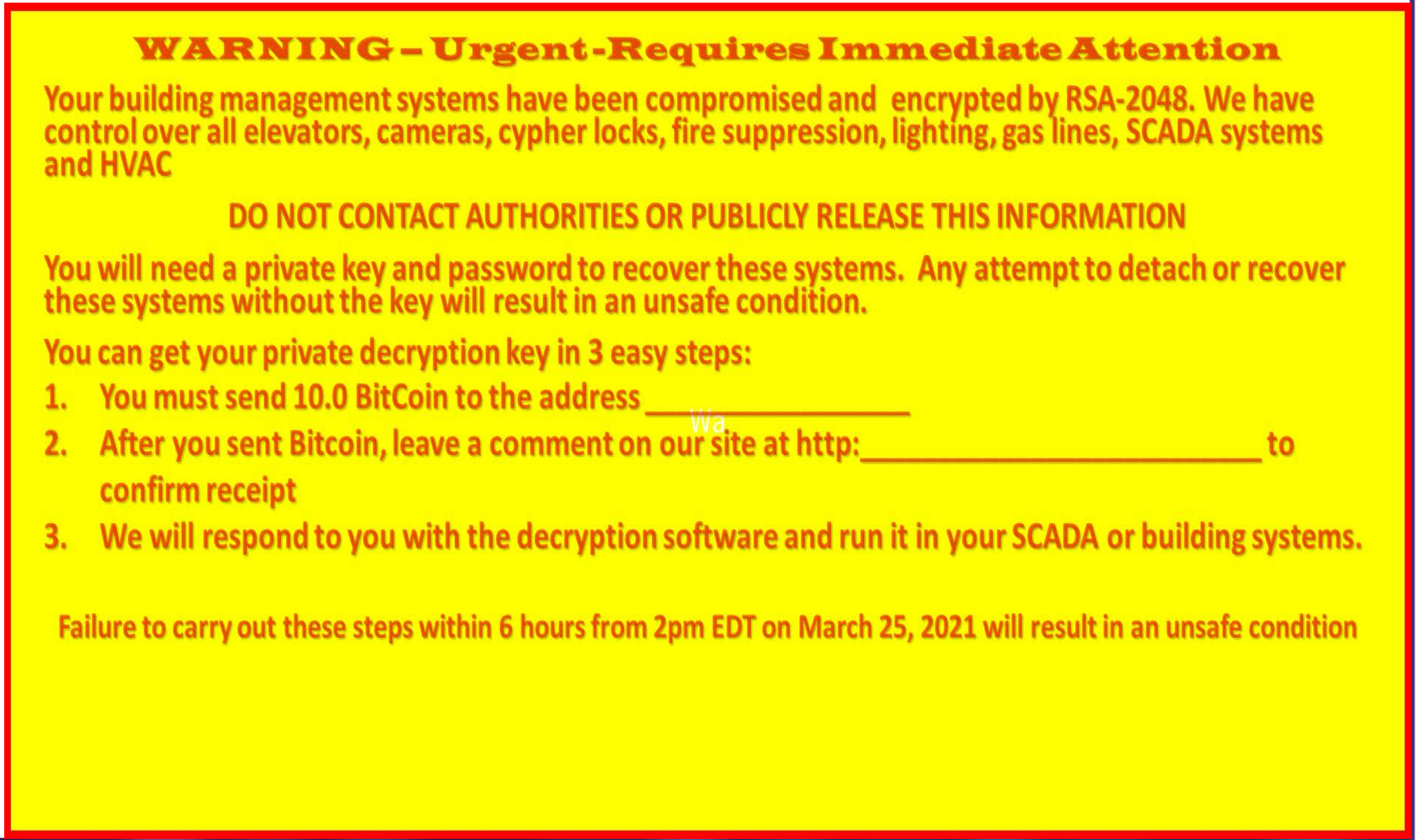


- A notice states that the New Krasnovian Cyborg Front has destroyed your systems and will win the inevitable victory over all those who aid the Republic of Pineland.

- All usable forensics are destroyed

OTHER REASONS FOR ATTACK

A Ransom Request will drive different courses of action from resources outside the installation and involvement of other federal agencies



WARNING – Urgent-Requires Immediate Attention

Your building management systems have been compromised and encrypted by RSA-2048. We have control over all elevators, cameras, cypher locks, fire suppression, lighting, gas lines, SCADA systems and HVAC

DO NOT CONTACT AUTHORITIES OR PUBLICLY RELEASE THIS INFORMATION

You will need a private key and password to recover these systems. Any attempt to detach or recover these systems without the key will result in an unsafe condition.

You can get your private decryption key in 3 easy steps:

1. You must send 10.0 BitCoin to the address ______________
2. After you sent Bitcoin, leave a comment on our site at http:_____________________ to confirm receipt
3. We will respond to you with the decryption software and run it in your SCADA or building systems.

Failure to carry out these steps within 6 hours from 2pm EDT on March 25, 2021 will result in an unsafe condition

THIS IS A CYBER ATTACK

The following checklist accounts for recommended actions to communicate, manage, mitigate, and respond to the incident

1. Conduct preliminary Damage Assessment
2. Determine COA's for human safety and building operations
3. Establish a local incident response command team
4. Coordinate with Cyber Incident Command
5. Determine Attack Vectors
6. Contain and Stabilize the incident
7. Develop and execute a recovery plan
8. Begin formal incident reporting CJCSM 6510.01B

Let's break these down in more detail

PRELIMINARY DAMAGE ASSESSMENT (DA)

Immediate Response with Joint Base Team for Bldg 1 Status

Observe and Orient as quickly as possible

- ❑ **Time to determine if other building systems are compromised**
- ❑ **Time to determine if there is a threat of compromise to the building's missions**
- ❑ **Mission impact of a building evacuation to protect human safety**
- ❑ **Intent of attacker**
- ❑ **Time to restore systems or install temporary equipment**

Decision by Joint Team

- ➢ **Safety - Continue Bldg 1 functions in place or evacuate building (short or long term)**
- ➢ **Mission Assurance**

BUILDING 1 COA'S

Initial Incident Response

- Safety of building personnel
- Impact if all data networks, connected devices, and building technologies are compromised
- Ability to transfer mission to another location
- Mission impact of evacuation
- Impact if computers and other connected devices remain in place
- Time to lock down and secure all sensitive areas
- Time to recover building

INSTALLATION COMMANDERS DAMAGE ASSESSMENT

TREATED AS A KINETIC ATTACK TO THE BASE

- Check **all** Building Management Systems in Bldg 1 for safety or compromise
- Check systems in other buildings based on mission criticality
- Extent of inventory of smart operational technologies
- Ability to confirm no compromise virtually?
- Confirm availability of critical Installation Support Functions
  - Base Access Control
  - Fire and emergency response
  - Flightline or other essential mission operations
  - Water/Wastewater, Utility/Steam Plants

Local IT/Comm office should be coordinating on incident response.

- **NIPR has different controls and safeguards than your FRCS Network**

DO NOT SHUT DOWN OR REBOOT ANY BUILDING AUTOMATION SYSTEMS

DAMAGE ASSESSMENT - EXAMINING CYBER ACCESS TO BLDG 1

Possible Attack Vectors within BCE Responsibility

- Remote access to a building system
- Zero-day discovery and activation in BMS
- Firmware, software, or patch flaw
- 3rd party vendor maintenance
- Unknown system connectivity to base network?
- Jumped a fire wall or air gap?
- Kinetic delivery

PRELIMINARY RESPONSE ACTIONS - DOCTRINE

The immediate steps taken once an incident has been detected and declared.

- These actions are important as they provide information to help protect the IS and information network from more damage while more detailed analysis is completed. These will be based on the nature, scope, and potential impact of the incident.
- The primary objectives of preliminary response include:
  - **Preventing** a reportable cyber event or incident from causing **further damage**.
  - **Maintaining control** of the affected system and the surrounding environment.
  - Ensuring **forensically sound acquisition of data** necessary.
  - **Maintaining** and updating the **incident report** and **actively communicating updates** through the appropriate technical and operational command channels.

CJCSM 6510.01B

LOCAL CYBER INCIDENT COMMAND RESPONSIBILITIES

Immediate **Isolation and Containment** is a Priority

1. Halt or minimize attack effects or damage while maintaining operational mission continuity.
2. Ensure the effective and timely recovery of ISs in a way that prevents similar incidents from occurring again.
3. Strengthen the Department of Defense's defensive posture and operational readiness.
4. Ensure that RAs occur in a manner that protects any data according to its level of sensitivity.
5. Support rapid, complete attack characterization.

From Enclosure E of CJCSM 6510.01B

COMMS SQUADRON RESPONSE

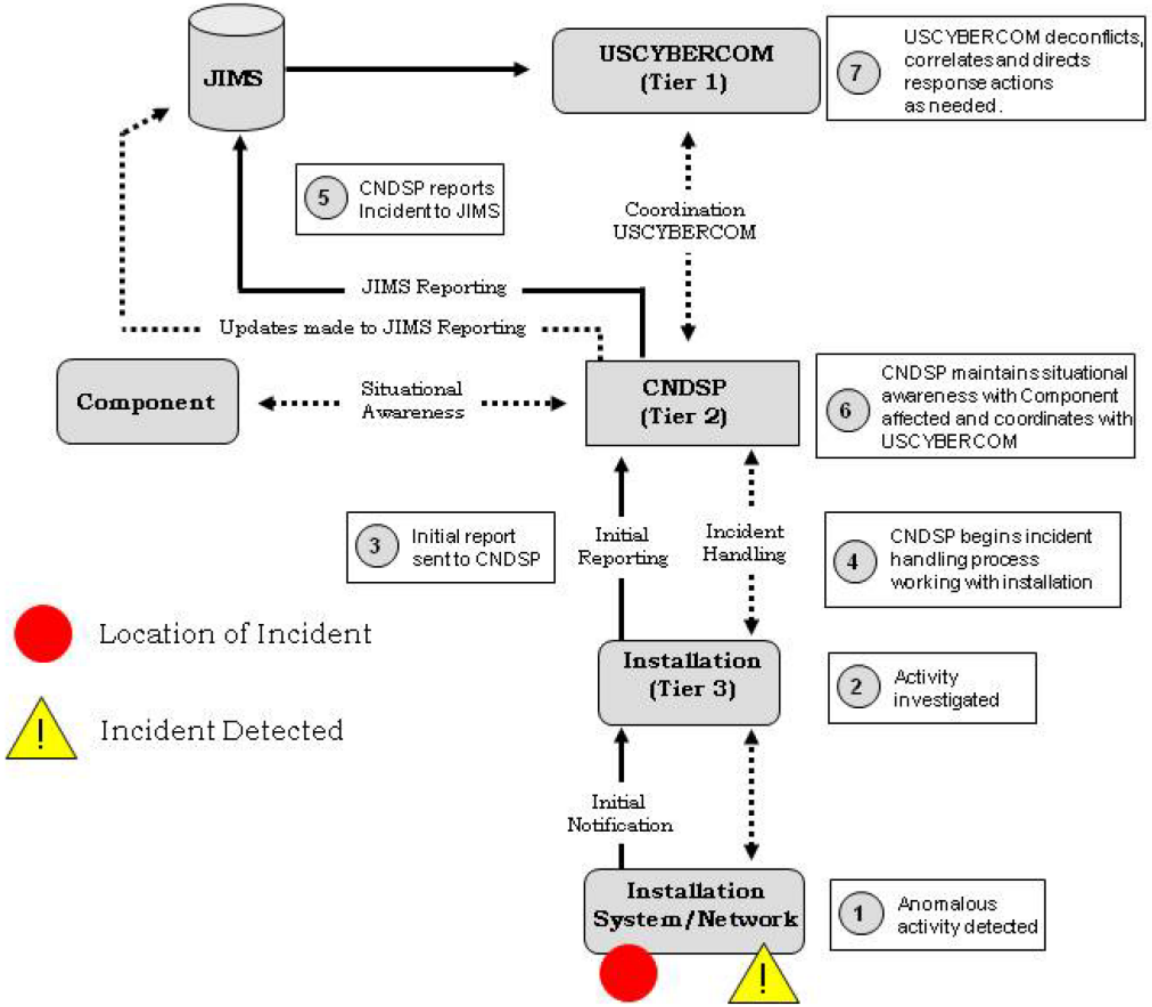
The Comm/ IT Team May NOT be familiar with OT

- Typical responses will be:
  - That's not our network. It's not NIPRNet or SIPRNet, so it belongs to a different office.

- They don't usually have visibility or access to the infrastructure network.
- They must be informed that an active cyber attack is going on, so that they can protect the networks under their responsibility, which are adjacent.
- You need their expertise in containment and remediation.

IMMEDIATE REPORTING REQUIREMENT

- Halt or minimize attack effects or damage while maintaining operational mission continuity.
- Ensure the effective and timely recovery of IS in a way that prevents similar incidents from occurring again.
- Strengthen the Department of Defense's defensive posture and operational readiness.
- Ensure that Response Actions occur in a manner that protects any data according to its level of sensitivity.
- Support rapid, complete attack characterization.



JIMS
USCYBERCOM (Tier 1)
7 USCYBERCOM deconflicts, correlates and directs response actions as needed.
5 CNDSP reports Incident to JIMS
Coordination USCYBERCOM
JIMS Reporting
Updates made to JIMS Reporting
Component
Situational Awareness
CNDSP (Tier 2)
6 CNDSP maintains situational awareness with Component affected and coordinates with USCYBERCOM
3 Initial report sent to CNDSP
Initial Reporting
Incident Handling
4 CNDSP begins incident handling process working with installation
● Location of Incident
⚠ Incident Detected
Installation (Tier 3)
2 Activity investigated
Initial Notification
Installation System/Network
1 Anomalous activity detected

CONTACTING THE SERVICE CSSP

The Service's Cyber Security Service Provider (CSSP), in this case AFCYBER, with authority over Installation networks provides the first external support.

- Your report to the CSSP starts the JIMS into motion.
- They will have network and local tools to begin to isolate, hunt, and respond appropriately to the cyber attack.
- Have their contact information on hand

JOINT INCIDENT MANAGEMENT SYSTEM (JIMS)

DOD’s central repository for managing event and incident reports.

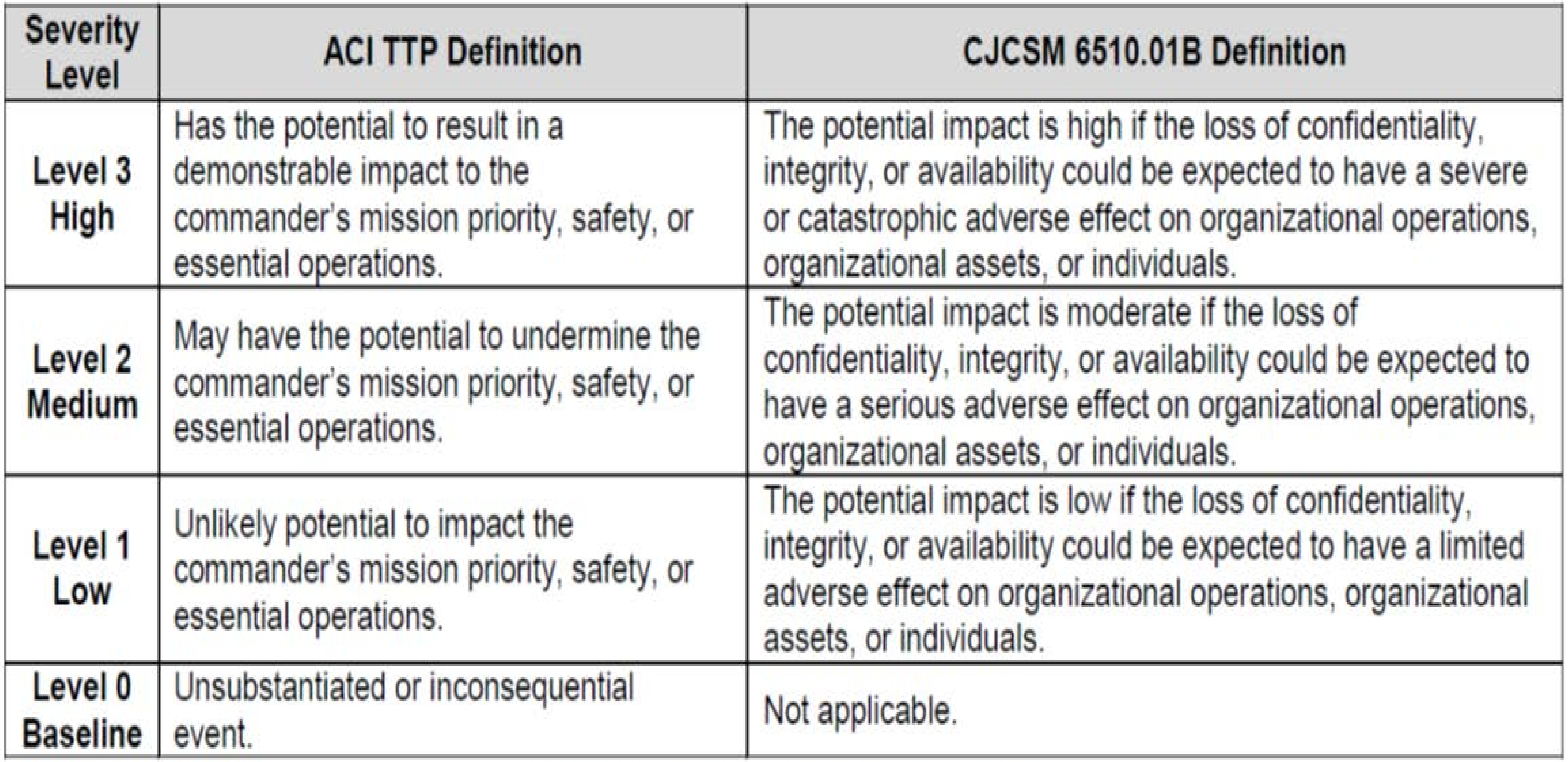
- Ensure the timely flow of crucial network intelligence across DoD/USG and ally boundaries to reflect the collective reporting of adversary actions, intentions, and capabilities; to assist in shaping tactical, strategic, and military response strategies; and to perform trending analysis, correlation, and fusion.
- The JIMS is used for recording possible foreign activity and domestic initiated threat activity suspected of being foreign in origin and against DoD networks.
- Use of the JIMS is required by the USCYBERCOM J2 and each Service component CERT/CIRT intelligence support element for the following categories of intrusions: (1) Category 1—Root Level Intrusion. (2) Category 2—User Level Intrusion. (3) Category 4—Denial of Service.
- Input into JIMS of initial analysis is required as soon as information becomes available. Initial analysis on an event should occur as soon as feasible.

REPORTING FOR CYBER INCIDENTS

CJCSM 6510.01B Cyber Incident Handling Program

Category	Impact	Initial Notification to Next Tier	Initial Report to Next Tier	Initial Submission to JIMS	Minimum Reporting
1 Root Level Intrusion* (Incident)	High	Within 15 Minutes	Within 4 Hours	Within 6 Hours	Tier I
	Moderate	Within 2 hours	Within 8 hours	Within 12 hours	Tier I
	Low	Within 4 hours	Within 12 hours	Within 24 hours	Tier I
2 User Level Intrusion* (incident)	High	Within 15 Minutes	Within 4 Hours	Within 6 Hours	Tier I
	Moderate	Within 2 hours	Within 8 hours	Within 12 hours	Tier I
	Low	Within 4 hours	Within 12 hours	Within 24 hours	Tier I
7 Malicious Logic (Incident)	High	Within 15 Minutes	Within 4 Hours	Within 6 Hours	Tier I
	Moderate	Within 2 hours	Within 8 hours	Within 12 hours	Tier II
	Low	As directed by CC/S/A/FA Guidance	As directed by CC/S/A/FA Guidance	As directed by CC/S/A/FA Guidance	Tier II

INCIDENT SEVERITY LEVELS



Severity Level	ACI TTP Definition	CJCSM 6510.01B Definition
Level 3 High	Has the potential to result in a demonstrable impact to the commander's mission priority, safety, or essential operations.	The potential impact is high if the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Level 2 Medium	May have the potential to undermine the commander's mission priority, safety, or essential operations.	The potential impact is moderate if the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
Level 1 Low	Unlikely potential to impact the commander's mission priority, safety, or essential operations.	The potential impact is low if the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
Level 0 Baseline	Unsubstantiated or inconsequential event.	Not applicable.

Table I-1: Incident Severity Levels

ONBOARD THE NATIONAL CYBER TEAM

Be prepared for the National Cyber Teams to come in person

- They will have a lot of tools and systems to put on the network.
- It's still your network, and you need to make sure they can quicky join it.
- They'll overwhelm your office spaces
- They will show up sooner than you expect
- **They are not under your control, and will take over your network until their work is done**

QUARANTINE AND STABILIZATION

How wide do we quarantine? –To the edge of the infection

- **Design** the system using segmented security **zones** with hardened and severable **conduits** – **before the incident**, to facilitate quarantine and triage
- Start at the installation and **work inward** to segment each major OT System and building.
- **Isolate** the building's network **physically**. (Unplug from the routers to other buildings)
- **Work with the COMM Squadron** to logically isolate all networked buildings, so they can be **cleared one by one**.
- Isolate each subsystem, (disconnect Fire Alarms from HVAC, from Access Control). Sub-system segregation
- Keep the systems running and, if possible, **take snapshots of the machine states.**Recording live machine states is very difficult on embedded systems.

PLC RECOVERY CONSIDERATIONS

What to Consider

- Keep PLCs in Read-Only configuration.
- **Physically disconnect** infected PLCs from network and sensors but **keep them powered on**.
- **Maintain back-up firmware and project images** with the latest patches and configurations, specific to the system.
- For critical systems, maintain replacement PLCs that can quickly replace damaged or infected ones, once the applicable security zone is cleared of malware and intrusions.
- **Practice routine and emergency** maintenance **procedures**, including response to cyber attacks.
- Know what contracting mechanisms exist
- Know how long it will take to restore.
- Know how much it will cost to restore.

AUDIENCE QUESTION

What needs to be done to restore Bldg 1 Operations?

How long would you estimate for restoration of building functions?

FORENSICS AND SYSTEM FAILURE ANALYSIS

Don’t be too quick to focus on a single “root” cause

- Know how to preserve artifacts so that Cyber, Safety, Intelligence Community, and Law Enforcement entities can accurately analyze the scene
- Don’t rush to blame. Let the Law Enforcement guys do that. As a base engineer, focus on systematic hazard analysis.
- There are often more than one underlying vulnerability or error. Don’t stop at the first one you spot.
- Use a cyclical hazard analysis model, such as MIT’s Causal Analysis based on System Theory (CAST) instead of a fault tree or other linear model

- Further Guidance – See ENCLOSURE G: DATA COLLECTION FOR FORENSICS of Advanced Cyber Industrial Control System Tactics, Techniques, and Procedures (ACI TTP) for Department of Defense (DoD) Industrial Control Systems

SYSTEM RESTORATION - REAL WORLD EXAMPLE

Day 2

- PC reformatted and OS reloaded
- Controllers, VFD, and equipment ordered
- Fresh copy of application installed

Day 3 -42

- Original programming installed
- Programming begins of the front-end rebuild system with program updates
- Controllers, VFD and VFD and other equipment are installed
- Original controller programming Installed
- Programming begins to rebuild controller program updates

Day 42-92

- Controller programming complete
- HVAC system inspection is completed
- System and cyber commissioning is conducted

INFECTION REMEDIATION

Does a Full Mission Capable (FMC) Network Exist?

- The FMC is a functional recovery point for both the ICS and the SCADA.
- ICS and IT managers should establish what a FMC network is as it pertains to their specific installations and missions.
- ICS and IT managers should capture the FMC condition of all network entry points (e.g., firewalls, routers, remote access terminals, wireless access points, etc.), network topology, network data flow, and machine/device configurations
- FMC must be stored in a secure location accessible if networks are down.
- FMC should be kept under configuration management and updated every time changes are made to the network.
- This information forms the FMC baseline used to determine normal operational versus anomalous conditions of the ICS.

DOES THE SYSTEM HAVE A JUMP-KIT READY TO GO?

A Recovery Jump-Kit contains the tools the ICS team and IT team will need to restore a system to its last FMC state during Mitigation and Recovery.

- Knowing what the Recovery point should be is the key to ensuring all known remnants of an attack have been removed from all components of the ICS and all hardware and software are configured in accordance with operational requirements, and checksums and hashes are in conformance with vendor specifications.
- Key Components
  1) Routine Monitoring
  2) Inspection
  3) Identification of adversarial presence
  4) Documentation
  5) Notifications
- Prerequisites. FMC baseline

Reference: Enclosure F: Jump Kit of Advanced Cyber Industrial Control System Tactics, Techniques, and Procedures (ACI TTP) for Department of Defense (DoD) Industrial Control Systems

JUMP KIT CONTENTS

The Jump-Kit is a critical tool for the Recovery phase

- In addition to containing the operating software for all devices, it also contains the software hashes of the devices on the network and the firmware and software updates for all system devices.
- During Recovery, the Jump-Kit will be utilized to reimage the firmware/software operating on the affected device.
- Care shall be used when the Jump-Kit machine is used for the reinstallation/reimaging potentially infected devices as malware residing on the device could manifest itself onto the Jump-Kit machine, which could then re-infect other system devices when reconnected.
- Due to this potential back door access for malware, ensure that the Jump-Kit machine is connected only to network devices that are completely isolated from the network.
- The Jump-Kit should be write-protected and/or operating in a virtual environment. Virus scans are performed after connection to each device.
- The ICS Jump-Kit and the IT Jump-Kit can be combined or be separate depending on the environment and system architecture.

JUMP-KIT CONTENTS: CONFIGURATION FILES

Must be confirmed with Installation IT Team

- Firewall access control lists
- Firewall hard disk image
- IDS rules
- IDS image
- Back up of firewall, router, and switch IOS
- Backup of PLC configurations and firmware
- Backup RTU software, database, and configurations
- Back up of all other computer assets to include HMI, Historian, and Database
- Network map of all expected connections to the ICS

Reference: Enclosure F: Jump Kit of Advanced Cyber Industrial Control System Tactics, Techniques, and Procedures (ACI TTP) for Department of Defense (DoD) Industrial Control Systems

HARDWARE REPLACEMENT

Is replacement hardware on site, is it planned for?

- Cyber attacks against OT systems have the potential to destroy physical hardware components.
- Repair and replacement of hardware for continued minimal mission operation and full mission capability must be part of the general disaster recovery plan and the expected response to a cyber attack.
- Hardware components are often difficult to reach or quickly repair, depending upon the nature of the system.

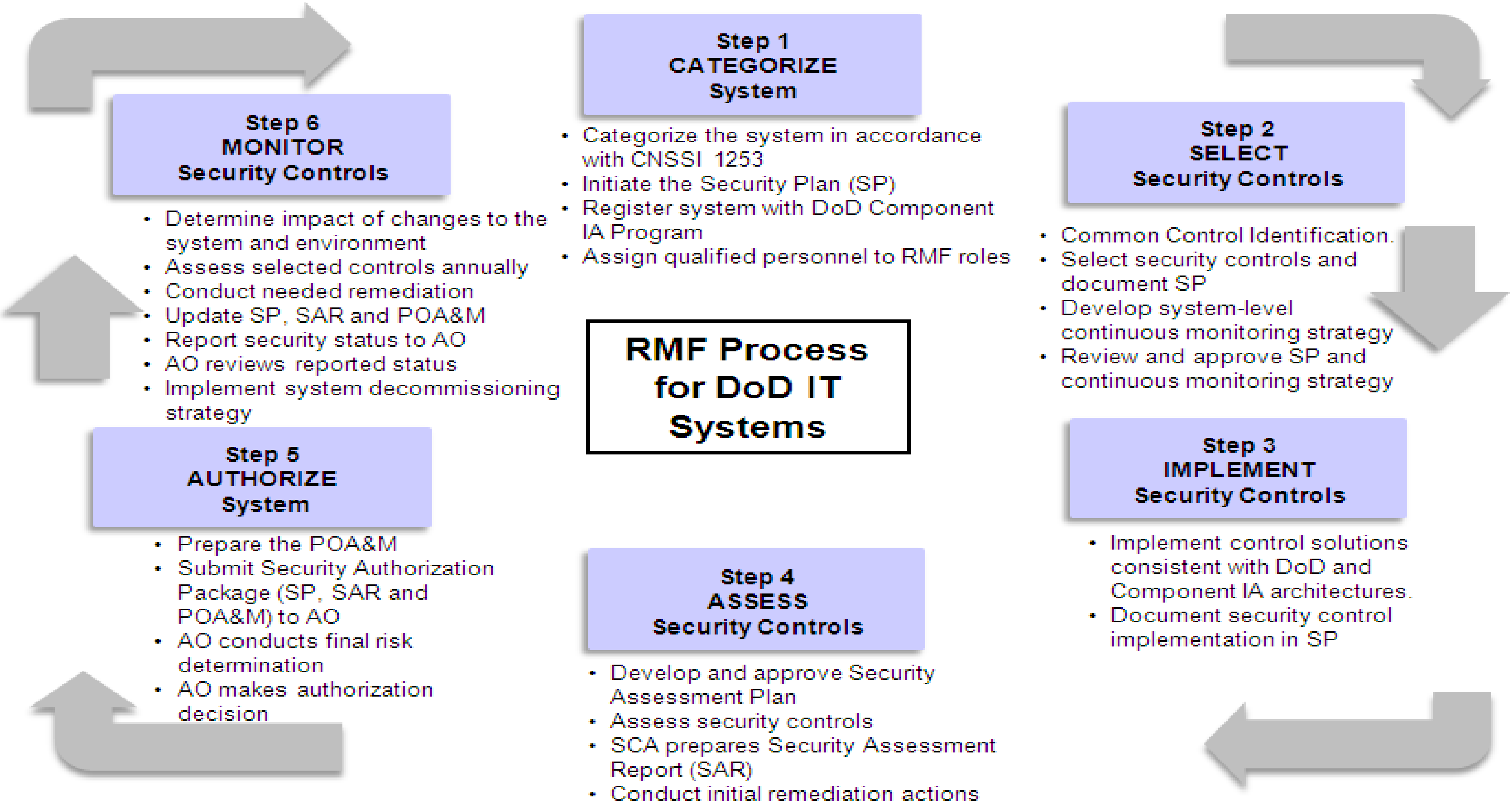
BUILDING RESTORATION

Reintegration of Building Systems must be slow and deliberate

- Once the initial incident response has occurred, the recovery process has to prevent reinfection of malware into the subsystems.
- Care must be taken to ensure that the Jump-Kits aren’t wasted or compromised during the rebuild.
- Utilizing the Zones and Conduits model from the ISA/IEC 62443 in the BAS architecture will facilitate a systematic, controlled rebuild and restoral of each security zone, and the subsystems with it, while reducing the risk of initial infection, and subsequent reinfection of other zones.

SEMINAR TAKE-AWAYS

RISK MANAGEMENT FRAMEWORK



RMF Process for DoD IT Systems

Step 1 CATEGORIZE System

- Categorize the system in accordance with CNSSI 1253
- Initiate the Security Plan (SP)
- Register system with DoD Component IA Program
- Assign qualified personnel to RMF roles

Step 2 SELECT Security Controls

- Common Control Identification.
- Select security controls and document SP
- Develop system-level continuous monitoring strategy
- Review and approve SP and continuous monitoring strategy

Step 3 IMPLEMENT Security Controls

- Implement control solutions consistent with DoD and Component IA architectures.
- Document security control implementation in SP

Step 4 ASSESS Security Controls

- Develop and approve Security Assessment Plan
- Assess security controls
- SCA prepares Security Assessment Report (SAR)
- Conduct initial remediation actions

Step 5 AUTHORIZE System

- Prepare the POA&M
- Submit Security Authorization Package (SP, SAR and POA&M) to AO
- AO conducts final risk determination
- AO makes authorization decision

Step 6 MONITOR Security Controls

- Determine impact of changes to the system and environment
- Assess selected controls annually
- Conduct needed remediation
- Update SP, SAR and POA&M
- Report security status to AO
- AO reviews reported status
- Implement system decommissioning strategy

OT SECURITY CAPABILITIES AND TOOLS

What can federal engineers implement now to reduce risk and mitigate threats?

- OT Threat Awareness
- End point detection and inventory
- Segmentation or micro-segmentation (leveraging SDN or related technologies)
- Continuous System monitoring
- OT network management
- Cyber gap assessment
- Recurring training
- Cyber commissioning
- Design instructions for new construction

CYBER GAP ASSESSMENTS

Intended for mission critical facilities with smart building systems

- Ideally conducted at design phase for review of proposed technology stacks, drawings, specifications, and other construction guidance for the use of operational technologies in the building
  - Brings together mission owners, design agents, and other entities identified installation to assess current cyber-related risks associated with connectivity, sensing/monitoring, segmentation, integration with IT, and cyber defense platforms/capabilities/performance over the life cycle of the building.
  - Crucial in the development of construction specifications and configurations instructions for installation of new equipment
  - Offers opportunity to design cyber security and safety into the networks and system architectures as opposed to "bolting" cyber protections after design

- Also available for existing facilities and military installations to determine systemic weaknesses and vulnerabilities in the OT
- Can include penetration testing, RMF review, patching protocols, unknown remote access
- Compliance with existing facility guidance and frameworks

ETHOS

OT-centric, open-source platform for sharing anonymous early warning threat information

- Publicly launched on April 24, 2023, ETHOS is a cooperative development in the OT security industry, with the goal of sharing data to investigate early threat indicators and discover new and novel attacks.
- The platform correlates security events across any number of end users regardless of the security solutions they use, requiring integration with security vendor technologies to send and receive correlated notifications.

Objectives

- Build an open-source codebase and platform for ETHOS' operational technology and industrial control system (OT/ICS) devices and networks for data sharing and collaboration
- Make innovative and egalitarian design and governance decisions
- Produce code that allows for early warning detections for cybersecurity teams and stakeholders, to benefit the cybersecurity community without seeking a profit

https://www.ethos-org.io/?mc_cid=d9bd2592d0&mc_eid=UNIQID

CYBERSECURITY COMMISSIONING

- A critical process for resiliency of DOD Facility-Related Control Systems in new buildings, modernization, and existing assets.
- Initial and recurring cybersecurity commissioning of increasingly smart facilities to maintain security, resiliency, efficiency, and occupant safety.
- Authority To Operate (ATO) certification for new and legacy FRCS, accountability for proper continuous monitoring and threat mitigation as required by the DoD 6 step Risk Management Framework (RMF) process for these systems .
- Factory Acceptance Testing (FAT)/Site Acceptance Testing (SAT)
- Should include requirements for continuous monitoring

AUDIENCE QUESTION

How effective are firewalls and airgaps between building system networks ?

FIREWALLS & OTHER DEVICES

Firewalls

- Protections
  - Rule Based Traffic Management
  - Explicit Deny
  - Intrusion Detection
- Limitations
  - Patching required (prone to vulnerabilities)
    - Can be hacked
    - Routing rules can be changed
  - Rules must be set (difficult to configure/setup)
  - Misconfiguration Common(Human Error)
    - Failure to Implement Tools
    - Unnecessary Services Enabled
  - Performs software-based segmentation

One Way Gateways/Data Diodes

- Protections
  - One-Way Traffic Only
    - Hardware Enforced
    - Eliminates Attack Opportunities
  - Definitive Network Segmentation
- Limitations
  - Can’t use for ICS Command and Control
    - Data Replication/ Data Historian use
    - Can’t route back through one-way enforcement
  - Data Diodes don’t assure data delivery
    - No synchronization
    - No Retransmission

“Air Gapped” Devices are not…

NETWORK DISCOVERY TOOLS

DoD CIO uses three primary tools to inventory and report on the status of IT and OT FRCS

- Enterprise Mission Assurance Support System (eMASS)
  - Web-based Government off-the-shelf solution that automates a broad range of services for comprehensive, fully-integrated cybersecurity management, including controls scorecard measurement, dashboard reporting, and the generation of Risk Management Framework (RMF) for DOD IT and DOD Information Assurance Certification and Accreditation Process (DIACAP) Package Reports.
  - eMASS provides an integrated suite of authorization capabilities and prevents cyber-attacks by establishing strict process control mechanisms for obtaining authority to connect information systems to DOD networks.
- The Defense Information Technology Repository Tool (DITPR)
- Select & Native Programming Data Input System for Information Technology (SNaP-IT).

Grass Marlin developed by NSA provides a method for discovering and cataloging SCADA and ICS systems on IP-based networks.

- Uses a variety of sources, including PCAP files, router and switch configuration files, CAM tables and live network packet captures
- The tool can automatically determine the available networks and generate the network topology as well as visualize the communication between hosts.
- Release Notes: https://github.com/iadgov/GRASSMARLIN Download: https://github.com/iadgov/GRASSMARLIN/releases/tag/v3.0.0

ICS CHARACTERIZATION

Establishing a Baseline

- Allows IT and ICS managers to document normal conditions for the ICS, and store these for reference during the execution of the Detection portion of the TTP.
- Without such information, Detecting the activity of an advanced cyber adversary would prove very difficult.
- The following artifacts should be included in the ICS baseline:
  - Network architecture diagram
  - Data flows
  - Authorized list of software and hardware
  - Configuration files
  - Firmware values
  - Authorized ports, protocols, and services
  - User accounts with authorized privileges.
- The baseline must be available even if the network is down

Reference: Appendix AA1: Site Characterization of Advanced Cyber Industrial Control System Tactics, Techniques, and Procedures (ACI TTP) for Department of Defense (DoD) Industrial Control Systems

SEGMENTATION STRATEGY

A documented process for understanding how your ICS assets could be separated during and after a cyber attack.

Each ICS environment is unique, based on protocols, network architecture, physical locations, equipment, software, and mission priorities.

1. Identify the commander's mission priorities. These are the most critical processes that must remain operational.
2. Identify critical processes and dependencies. This includes identifying all of the assets that are required to keep the mission priorities operational.
3. Review the network architecture to identify logical points where segmentation could occur to contain infected assets or protect the ICS processes.

This document should be maintained with the continuity of operations and baseline documentation.

Reference: Enclosure H: Mitigation Isolation and Protection of Advanced Cyber Industrial Control System Tactics, Techniques, and Procedures (ACI TTP) for Department of Defense (DoD) Industrial Control Systems and Industry Standard (ICS)ISA/IEC 62443 Series

ZONES AND CONDUITS SEGMENTATION

Separate OT and ICS based on zones and conduits.

- Zone segmentation is the division of industrial systems into grouped sub-systems for the primary purpose of reducing the attack surface and minimizing attack vectors. It limits the flow of data between zones.
  - Physical zones are defined based on the grouping of assets based on physical location.
  - Logical zones are grouped based on a particular functionality or characteristic.
- Sub-system segmentation is meant to assist operators in isolating a targeted or affected sub-system or function.
  - The three main segments of an ICS are field devices, field controllers, and HMIs.
  - The purpose of sub-system Mitigation is to isolate and maintain local control of a particular function without affecting the remainder of the system.

Reference: Enclosure H: Mitigation Isolation and Protection of Advanced Cyber Industrial Control System Tactics, Techniques, and Procedures (ACI TTP) for Department of Defense (DoD) Industrial Control Systems and Industry Standard (ICS)ISA/IEC 62443 Series

ENGINEER TRAINING

CISA's Virtual Learning Portal in collaboration with INL, offers 100 & 200 level courses virtually, and 300 & 400 on-site free of charge:

- 100W - Operational Security (OPSEC) for Control Systems - This training is intended for anyone working in a control system environment. (1 hr)
- 210W - Cybersecurity for Industrial Control Systems - This course is an online-web based version of ICS 101 and 201 instructor-led courses. The course contains modules covering many aspects of cybersecurity for industrial control systems. (15 hr)
- https://ics-training.inl.gov/learn/signin

SANS offers ICS410 – GISCP and ICS515 – GRID

- https://www.sans.org/industrial-control-systems-security/

ISA Training on 62443 (IC32, IC33, IC34, IC37) and Certified Automation Professional

- https://www.isa.org/certification/certificate-programs/isa-iec-62443-cybersecurity-certificate-program
- https://www.isa.org/certification/cap

Other Resources –

- Whole Building Design Guide – Cyber Security

- https://www.wbdg.org/resources/cybersecurity

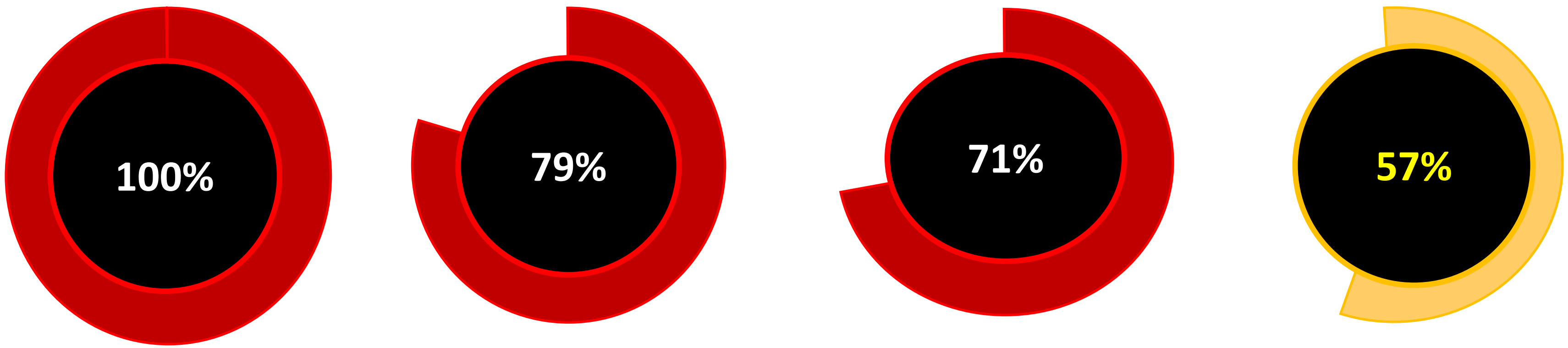
- SERDP-ESTCP FRCS Training

- https://serdp-estcp.org/toolsandtraining/details/377d0819-38d9-4d1d-a7e9-d8ada43c3f70

CONTROL SYSTEMS CYBER HYGIENE AUDIT REPORTS

- **Objective: Determine whether unit personnel implemented control system cyber hygiene practices IAW with Service Guidance**

*** illustrative examples**



Scanning Tools

Outdated SCAP tools

Plans

Unaware of preparing & testing plans

eMASS

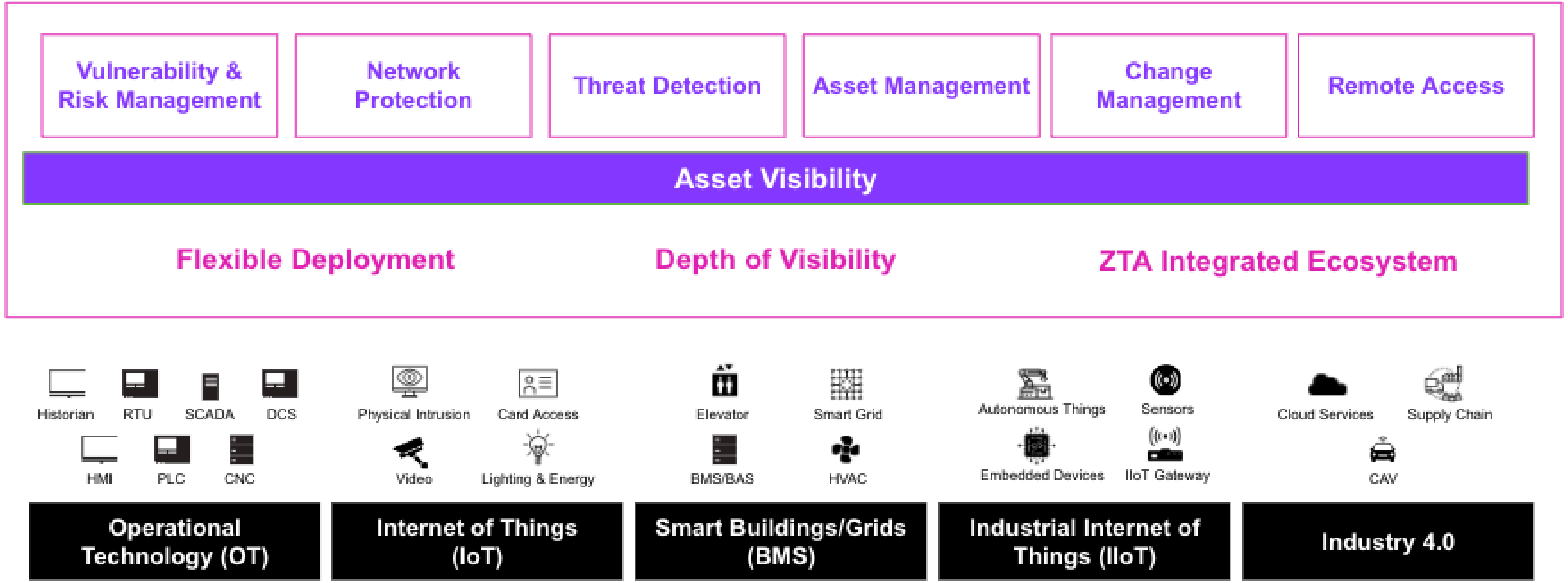
Did not update eMASS with required system documentation

Training

Did not complete PME

Conclusion: Did NOT implement IAW guidance

Recommendation: Leverage Solutions With a Holistic Approach to ICS Security



Vulnerability & Risk Management | Network Protection | Threat Detection | Asset Management | Change Management | Remote Access

Asset Visibility

Flexible Deployment | Depth of Visibility | ZTA Integrated Ecosystem

Operational Technology (OT) | Internet of Things (IoT) | Smart Buildings/Grids (BMS) | Industrial Internet of Things (IIoT) | Industry 4.0

FINAL THOUGHTS

- Facility teams must be trained to consider and recognize a cyber attack
- Responding to an OT cyber attack must consider an immediate threat to human safety
- Facility Engineers must review and practice TTPs with IT and network staffs
- Facility engineers must maintain inventories of smart building systems and FMC capabilities
- Installation IT teams must recognize and protect the OT on networks
- Facility engineers must provide clear guidance to manufacturers and maintainers on the configurations of digital components in building systems
- Facility engineers must be trained on established processes for cyber response
- Facility engineers must invest in protections and risk mitigation to OT systems

EXERCISE DEBRIEF

EXERCISE DEBRIEF

- Takeaway Questions:
  - What are your key takeaways from this event?
  - What choices of action presented the greatest challenges? Why?
  - If a similar scenario were to happen in your installation, what additional key decisions would need to be considered?
  - How do installations and communities protect themselves from attacks like this in the future?
  - Given your experience in today’s event, how might you take what you learned today to change your installation’s preparedness posture?

THANK YOU!

OUTBRIEF TO EAG

Warfighter Seminar #2

Mission Recovery from a Cyber Physical System (CPS) Attack to a Domestic National Security Asset

Warfighter Seminar #2 - Participating Organizations

1898 & CO
PART OF BURNS & McDONNELL

HDR

RMC
ASSURING TOMORROW

VISIONEERIT

ALETA
Technologies

Michael Baker
INTERNATIONAL

Booz | Allen | Hamilton®

NAVFAC

DEPARTMENT OF THE AIR FORCE
UNITED STATES OF AMERICA
MCMXLVII

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

UNITED STATES NORTHERN COMMAND

UNITED STATES STRATEGIC COMMAND

UNITED STATES CYBER COMMAND

TETRA TECH

The PMC Group LLC
Engineering a better tomorrow today

LUTRON®

PARSONS

U.S. INDO-PACIFIC COMMAND

UNITED STATES SPACE COMMAND

US Army Corps
of Engineers®

UNITED STATES CENTRAL COMMAND

Chinook

Salas O'Brien

NOZOMI
NETWORKS

CLAROTY

Seminar #2: Mission Recovery from a Cyber Physical System (CPS) Attack to a Domestic National Security Asset

Seminar Moderator: Lucian Niemeyer, CEO Building Cyber Security
Seminar Co-Leader: David A. Forbes, Principal, Booz | Allen | Hamilton
Seminar Co-Leader: Daryl Haegley, SL, GICSP,OCP Department of the Air Force Technical Director, DAF Control Systems Cyber Resiliency
Seminar Co-Leader: Brian May, Senior Vice President - Air Force Market Lead, Michael Baker International

Panelists

Government

HQ NAVFAC
US Army Corps of Engineers
US SPACE COMMAND
US NORTHERN COMMAND
US INDOPACIFIC COMMAND

US CENTRAL COMMAND
NFEXWG
US STRATCOM
NSA
US CYBERCOM

Industry

Aleta Technologies
Chinook Systems
Claroty
HDR
Lutron
Nozomi Networks
1898

Salas O’Brien
TetraTech
RMC
PMC Group
VisioneerIT
Parsons

Seminar #2: Mission Recovery from a Cyber Physical System (CPS) Attack to a Domestic National Security Asset

Description: National Defense Strategies have noted that the homeland is no longer a sanctuary. America is a target, whether from terrorists seeking to attack our citizens; malicious cyber activity against personal, commercial, or government infrastructure; or political and information subversion. Increasing digital connectivity of all aspects of life, business, government, and military creates significant vulnerabilities. During conflict, attacks against our critical defense, government, and economic infrastructure must be anticipated.

Using a designed scenario specifically targeting a mission essential building system at a notional military asset to deny a national security mission, the panel will discuss the processes and protocols needed by military engineers to meet federal guidance to quickly identify, protect, detect, respond, and recover from a cyber-physical attack. The scenario will highlight the operational technology mapping requirements for national security critical assets required by Congress via Sec 1505 of the National Security Authorization Act for Fiscal Year 2022.

The discussion will focus on roles and responsibilities of building systems military, industry, and contractor stakeholders to mitigate the risk and impact of a cyber attack, spanning from building design through continuous facility operations. The seminar will review and/or develop tactics, techniques, and procedures to immediately respond to and recover essential mission functions. The scenario includes input from building system manufacturers, supply chain specialists, facility designers, facility operators, and cyber security experts, providing engineers unique insights and a comprehensive understanding of the risks.

Seminar #2: Mission Recovery from a Cyber Physical System (CPS) Attack to a Domestic National Security Asset

Learning Objectives:

- Review processes to identify critical systems and cyber vulnerabilities within a risk management framework;
- Identify proactive measures to protect critical systems and mitigate risk of a cyber physical attack;
- Present methods to detect and confirm the origin and method of a cyber attack and damage assessment;
- Develop checklists and protocols to quickly isolate, respond and communicate progress to the incident;
- Assess options, probabilities and timing for the recovery missional essential system; and
- Identify programs to share information within the National Security command structure on the incident

FINDINGS/RECOMMENDATIONS

- Facility teams must be trained to consider and recognize a cyber attack
- Responding to an OT cyber attack must consider an immediate threat to human safety
- Facility Engineers must review and practice TTPs with IT and network staffs
- Facility engineers must maintain inventories of smart building systems and FMC capabilities
- Installation IT teams must recognize and protect the OT on networks
- Facility engineers must provide clear guidance to manufacturers and maintainers on the configurations of digital components in building systems
- Facility engineers must be trained on established processes for cyber response
- Facility engineers must invest in protections and risk mitigation to OT systems

Seminar #2: Mission Recovery from a Cyber Physical System (CPS) Attack to a Domestic National Security Asset

Findings and Recommendations

Finding #1: Training and awareness is lacking on impact of cyber on OT systems

Recommendation: Cyber attack and defense needs to be integrated into curriculum for PME for engineering community. Initial training pipelines need to include this for both enlisted and officers. The EAG should formally invite their cyber counterparts to a shared forum.

Finding #2: Decision process at first response call center in order to deduce response time for decision makers

Recommendation: Incorporation of cyber as a potential root cause to drive troubleshooting questions and notification of Comms and CSSP in SOPs. Characterization of extent of impact.

Finding #3: A cyber attack on/to OT should be treated as kinetic attack

Recommendation: Establish Roles and Responsibilities for initial Damage Assessment and declaration of building safety and incident response, including Deny, Destroy, Disrupt, Delay, and Deceive.

Finding #4: There is not enough information sharing across the Services

Recommendation: Establishment or restoration of a Cross-Service WG to innovate and standardize OT response, including use of MOSAICS, CRADA’s and other similar frameworks.

Seminar #2: Mission Recovery from a Cyber Physical System (CPS) Attack to a Domestic National Security Asset

Findings and Recommendations

Finding #5: Annual Installation TTX and Facility TTX are not being implemented

Recommendation: Incorporate Cyber Evaluations into formal Mission Readiness Inspections and reinforce the necessity for installation TTXs to include all installation support functions, (i.e. PA, IT/Comms, Contracting), within an installation response team.

Finding #6: MILCON and Facilities Acquisition contracts are not currently spec'd with OT Cyber and an RMF ATO

Recommendation: Amend the definition of a complete and usable facility to include an authority to operate for all systems.

Finding #7: Current direction, guidance, and policy for OT cybersecurity are not understood or implemented at installation levels

Recommendation: Train O&M teams and Project Management teams on OT Cyber threats and requirements.

Seminar #2: Mission Recovery from a Cyber Physical System (CPS) Attack to a Domestic National Security Asset

Findings and Recommendations

Finding #8: Concern that Installations don’t have a full inventory of connected systems, current Full Mission Capable (FMC) baselines, Jump Kit Toolsets, and update procedures.

Recommendation: Emphasize the requirement to have these back-up systems for mission critical facilities.

Finding #9:

Recommendation:

Senior Leader Comments

Mr. Mike McAndrew, OSD

MG Kimberly Colloton, USACE

RADM Dean VanderLey, NAVFAC

MG Thomas Tickner, IMCOM

BG Brian Hartless, USAF

CAPT John Barresi, USCG

RADM Emil Wang, USPHS

Dr. Mike Brennan, VA

Mr. John Pitts, OBO, DoS