

The PMC Group LLC

Engineering a better tomorrow today



DoD Cybersecuring Facility-Related Control Systems

Michael Chipley, PhD GICSP PMP
President

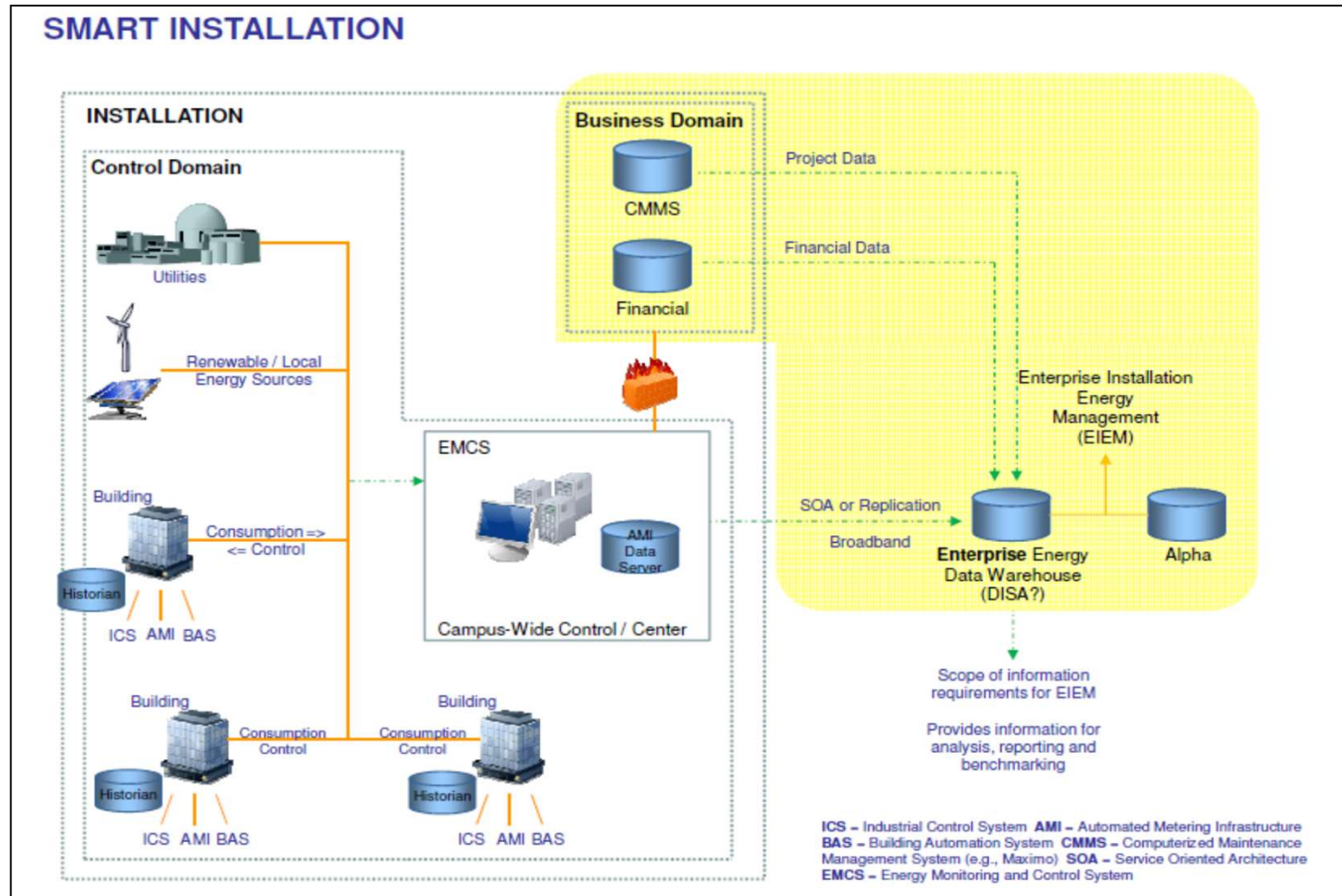
mchipley@outlook.com

February 20, 2025

Abstract

Over the past decade, the DoD has implemented Cybersecuring Facility-Related Control Systems to protect these Critical Infrastructure systems from adversaries and malicious actors. This presentation will review the history of how the program came to be and some key milestones such as the release of the first Cybersecurity Design Unified Facility Criteria, the first Construction Unified Facility Guide Specification, and the need for qualified Cybersecurity Subject Matter Experts and Specialists. **The session will provide hands on examples of the types of control systems, how the design criteria and construction specifications are used, and what the Cyber Team does to include provisioning and hardening the components and devices, capturing the Configuration Baseline Audit Report and Artifacts, and preparing the Cyber Submittals to obtain an Authority To Operate.** Similar to many of the ISSA activities for IT systems, the Control Systems now use traditional IT components and devices and the NIST SP 800-53, but now use NIST SP 800-82 to address the unique challenges of securing Operational Technologies such as Combined Heat Power Plants, Microgrids, HVAC, Fire, Lighting and Electronic Security Systems. ISSA members looking to expand their skill sets and become an OT Cyber Specialist will find a number of opportunities awaiting, this session is the introduction to get you started on the path to becoming a Cyber Warrior.

In the Beginning – Smart Installations



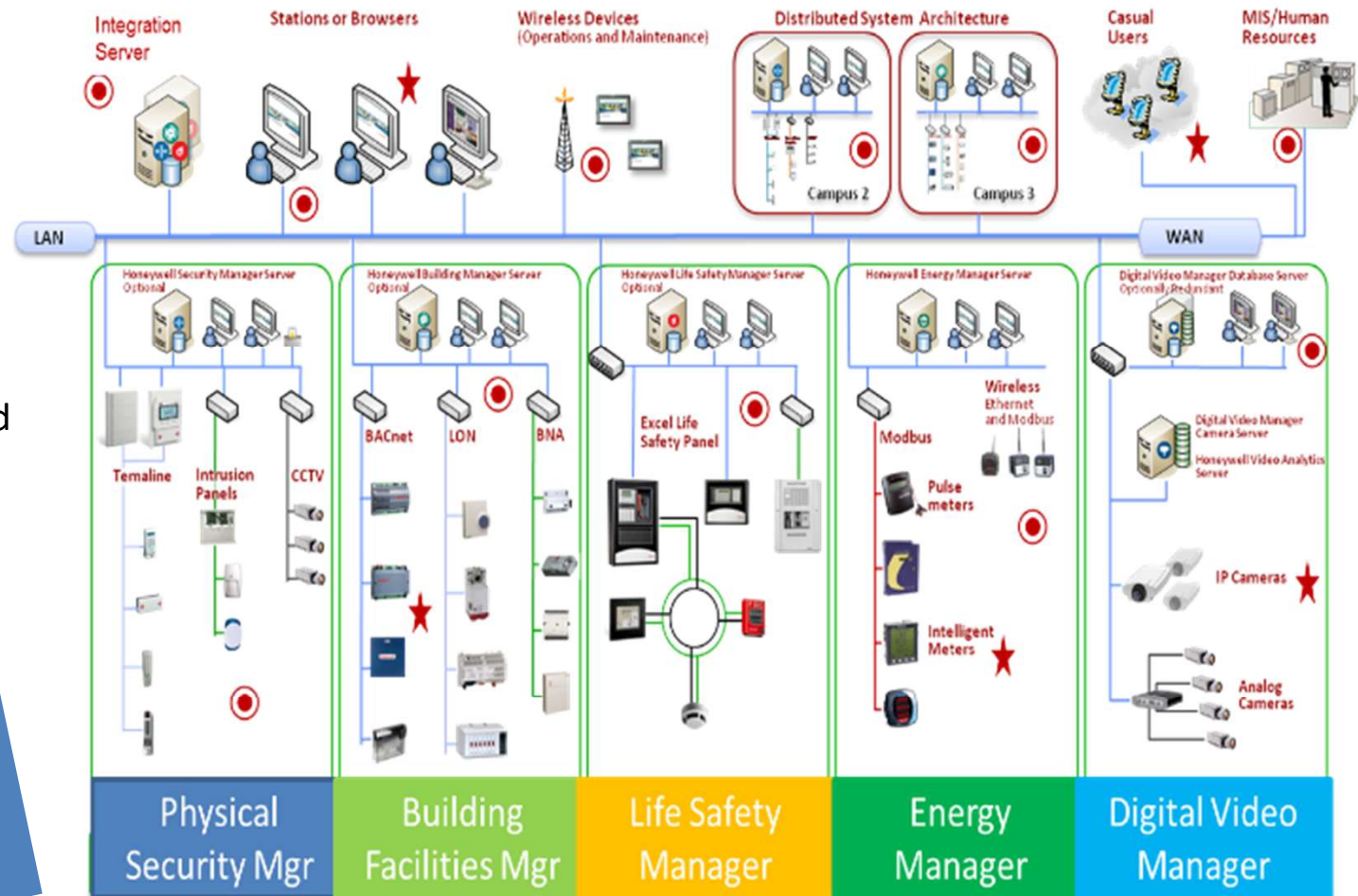
A great idea rudely interrupted by reality...CIO AMI ATO denial,... Stuxnet attack on Iranian Centrifuges, Flame, Duqu, Shamoon....

DoD Building FRCS

DoD Real Property Portfolio

- 48 countries
- 523 installations
- 4,855 Sites
- 562,600 buildings and structures
- 24.7 M acres
- \$847 B value

What's in Your Building?




★ Possible entry point of attack ● Potential compromise


OT IP Based Controllers Are in Everything

UNCLASSIFIED


Buildings




Weapon Platforms




Tactical




Electrical and HVAC




Nuclear




Medical




Controller



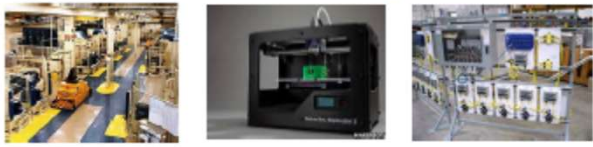
Pumps and Motors



Electric Vehicles/Charging



Manufacturing



Same Commercial Device Installed Across DoD Enterprise; PIT & PIT Systems

Shodan

The screenshot shows the Shodan website homepage. At the top, there is a navigation bar with links for Shodan, Maps, Images, Monitor, Developer, and More... Below this is a search bar with the placeholder text "Type / to search" and a red search button. A green "Login" button is located in the top right corner. The main content area features a large heading "Search Engine for the Internet of Everything" and a sub-heading "Shodan is the world's first search engine for Internet-connected devices. Discover how Internet intelligence can help you make better decisions." Below the text is a green "SIGN UP NOW" button. To the right of the text is a world map with a heatmap overlay showing data points. Below the main content area is a section titled "// EXPLORE THE PLATFORM" with three columns of featured content: "Beyond the Web", "Monitor Network Exposure", and "Internet Intelligence".

Shodan

Explore Pricing ↗ Type / to search Login

Search Engine for the Internet of Everything

Shodan is the world's first search engine for Internet-connected devices. Discover how Internet intelligence can help you make better decisions.

[SIGN UP NOW](#)

// EXPLORE THE PLATFORM

- Beyond the Web**
Websites are just one part of the Internet. Use Shodan to discover everything from power plants, mobile phones, refrigerators and
- Monitor Network Exposure**
Keep track of all your devices that are directly accessible from the Internet. Shodan provides a comprehensive view of all exposed services
- Internet Intelligence**
Learn more about who is using various products and how they're changing over time. Shodan gives you a data-driven view of the

Our joint job is to make sure no DoD Systems show up on Shodan

[Shodan Search Engine](https://www.shodan.io)

Shodan Rockwell Bradley

The screenshot shows the Shodan search interface for the query 'rockwell bradley'. The browser address bar shows the URL 'https://www.shodan.io/search?query=rockwell+bradley'. The search bar contains 'rockwell bradley' and a search button. The page displays 6,466 total results. On the left, there are sections for 'TOTAL RESULTS', 'TOP COUNTRIES' (with a world map), and 'TOP PORTS'. The main content area shows a 'Product Spotlight' and a list of search results. Each result includes an IP address, a vendor name, product name, vendor ID, serial number, device type, and device IP. The results are sorted by IP address.

Browser address bar: <https://www.shodan.io/search?query=rockwell+bradley>

Search bar: rockwell bradley

Navigation: Shodan, Maps, Images, Monitor, Developer, More...

Shodan logo, Explore, Pricing, Login

TOTAL RESULTS: 6,466

TOP COUNTRIES

Country	Count
United States	4,378
Canada	575
Spain	239
Italy	170
Australia	146
More...	

TOP PORTS

Port	Count
44818	6,433
2003	4
2004	3
502	2

Product Spotlight: We've Launched a new API for Fast Vulnerability Lookups. Check out [CVEDB](#)

107.84.240.246 2024-09-05T20:28:44.885487

AT&T Mobility LLC
United States, Lincoln

ICS

Product name: 1769-L24ER-QBFC1B/A LOGIX5324ER
Vendor ID: Rockwell Automation/Allen-Bradley
Serial number: 0xc01b8175
Device type: Programmable Logic Controller
Device IP: 192.168.1.10

166.136.164.19 2024-09-05T12:47:42.346602

mobile-166-136-164-019.mycingular.net
Wireless Data Service Provider Corporation
United States, Glendale

ICS

Product name: 1766-L32AWA C/21.02
Vendor ID: Rockwell Automation/Allen-Bradley
Serial number: 0xd050d191
Device type: Programmable Logic Controller
Device IP: 192.168.100.2

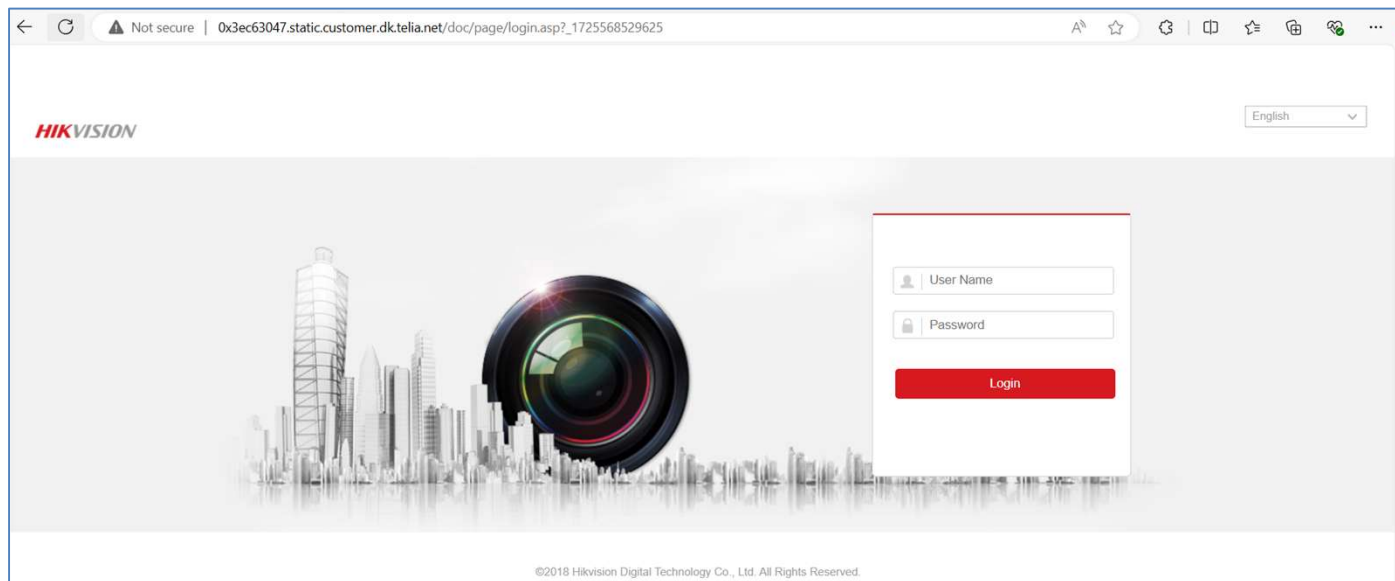
63.46.1.66 2024-09-05T12:19:42.745040

host66.sub-63-46-1.myvzw.com
Verizon Business
United States, Baldwin

ICS

Product name: 1766-L32BXBA C/21.07
Vendor ID: Rockwell Automation/Allen-Bradley
Serial number: 0x60f099c9
Device type: Programmable Logic Controller
Device IP: 192.168.13.100

Shodan HMI Logins



Shodan DoD

192.63.80.11
syn-192-063-080-011.res.spectrum.com
Charter Communications
United States, Killen

eol-os self-signed

SSL Certificate
Issued By:
|- Common Name: HOODRRMWRSPR04

Issued To:
|- Common Name: HOODRRMWRSPR04

Supported SSL Versions:
TLV1, TLSv1.1, TLSv1.2

Diffie-Hellman Fingerprint:
RFC2409Oakley Group 2

Vulnerabilities
BlueKeep

2024-09-05T17:23:36.596250

Remote Desktop Protocol
\\x03\\x00\\x00\\x13\\x0e\\x00\\x00\\x124\\x00\\x02\\t\\x00\\x00\\x02\\x00\\x00

Remote Desktop Protocol NTLM Info:
OS: Windows 7/Windows Server 2008 R2
OS Build: 6.1.7601
Target Name: HOODRRMWRSPR04
NetBIOS Domain Name: HOODRRMWRSPR04
NetBIOS Computer Name: HOODRRMWRSPR04...

152.179.117.114
Internet-gw.customer.alter.net
Verizon Business
United States, Jessup

CC

THIS IS A DEPARTMENT OF DEFENSE (DOD) INTEREST COMPUTER SYSTEM. ALL DOD INTEREST COMPUTER SYSTEMS AND RELATED EQUIPMENT ARE INTENDED FOR COMMUNICATION, TRANSMISSION, PROCESSING, AND STORAGE OF OFFICIAL U.S. GOVERNMENT ...

2024-08-29T23:49:50.286343

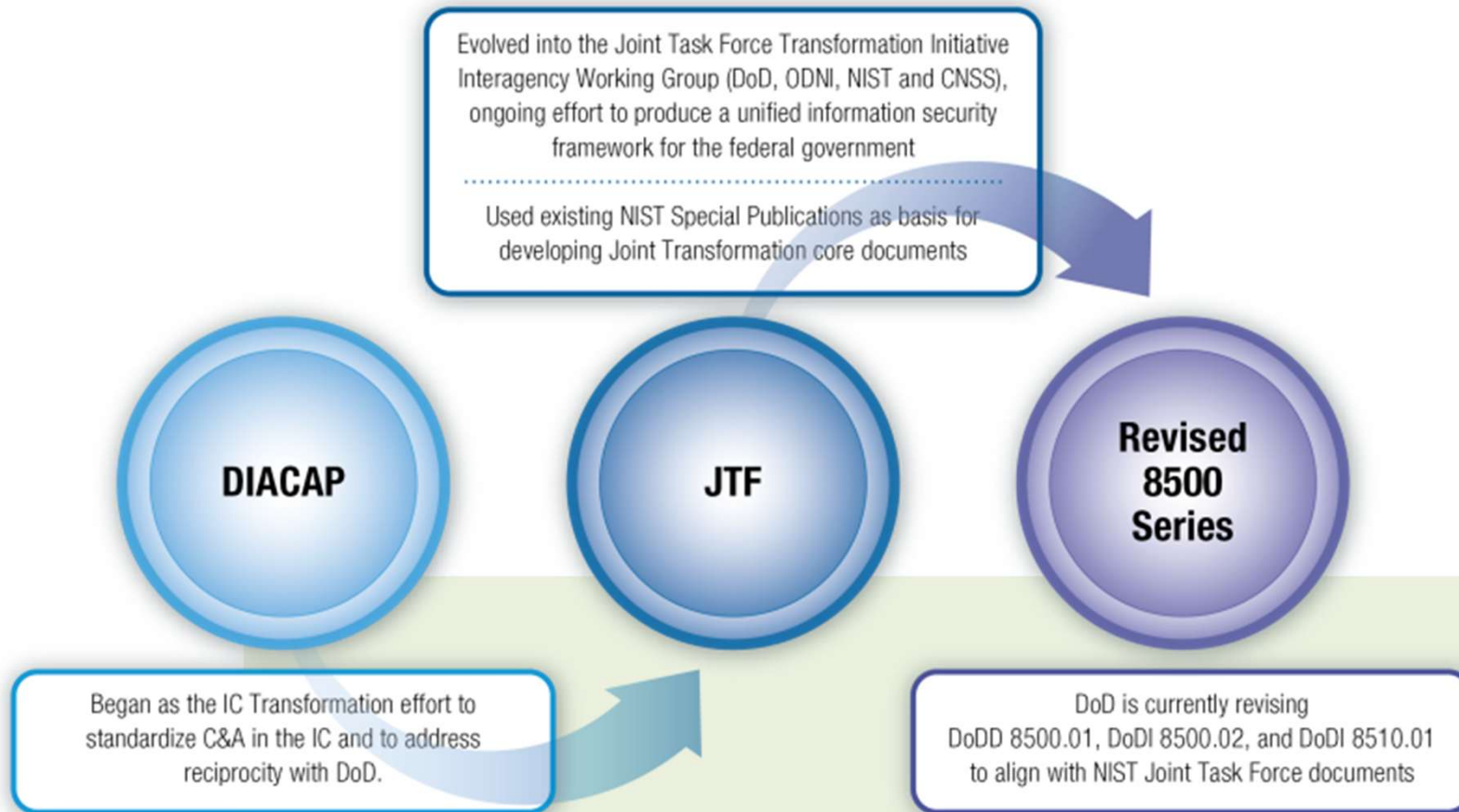
65.199.61.70
Verizon Business
United States, Washington

CC

THIS IS A DEPARTMENT OF DEFENSE (DOD) INTEREST COMPUTER SYSTEM. ALL DOD INTEREST COMPUTER SYSTEMS AND RELATED EQUIPMENT ARE INTENDED FOR COMMUNICATION, TRANSMISSION, PROCESSING, AND STORAGE OF OFFICIAL U.S. GOVERNMENT ...

2024-08-29T15:03:16.956223

DoDI 8500.01 and 8510.01 Update



Transition Bottom Line – DoD will continue to follow the DoD 8500 series documentation for information assurance and risk management processes, procedures, and guidance

8500 PIT Cybersecurity Considerations

(2) PIT

(a) All PIT has cybersecurity considerations. The Defense cybersecurity program only addresses the protection of the IT included in the platform. See Reference (ah) for PIT cybersecurity requirements.

(b) Examples of platforms that may include PIT are: weapons, training simulators, diagnostic test and maintenance equipment, calibration equipment, equipment used in the research and development of weapons systems, medical technologies, vehicles and alternative fueled vehicles (e.g., electric, bio-fuel, Liquid Natural Gas that contain car-computers), **buildings and their associated control systems (building automation systems or building management systems, energy management system, fire and life safety, physical security, elevators, etc.), utility distribution systems (such as electric, water, waste water, natural gas and steam), telecommunications systems designed specifically for industrial control systems to include supervisory control and data acquisition, direct digital control, programmable logic controllers, other control devices and advanced metering or sub-metering**, including associated data transport mechanisms (e.g., data links, dedicated networks).

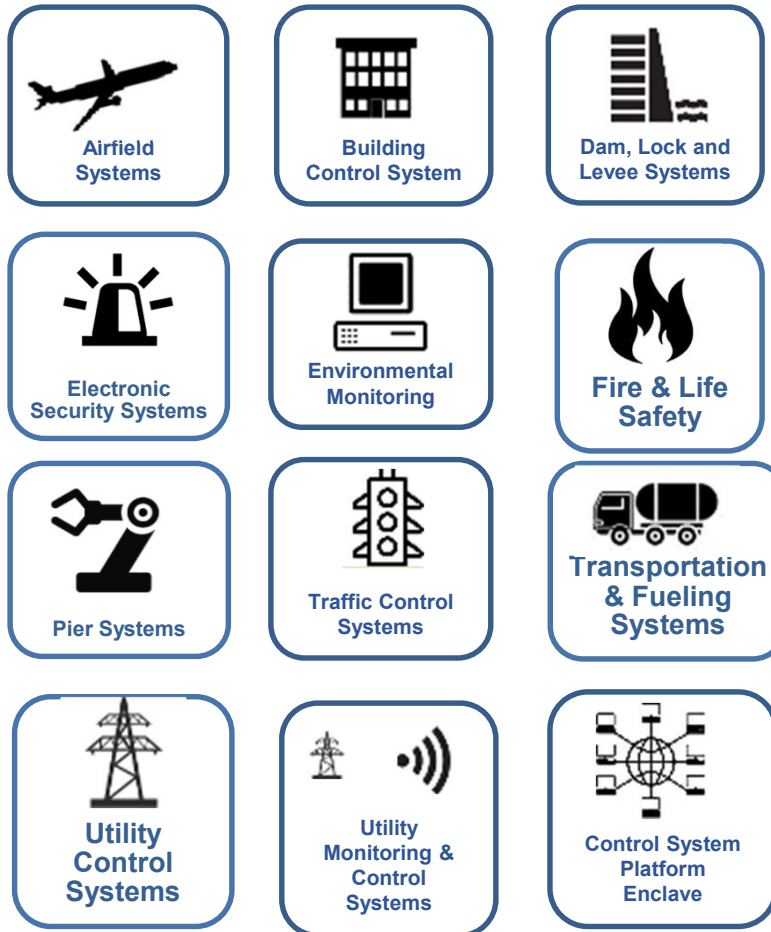
8500 PIT Systems

(d) PIT Systems

1. Owners of special purpose systems (i.e., platforms), in consultation with an AO, may determine that a **collection of PIT rises to the level of a PIT system. PIT systems are analogous to enclaves but are dedicated only to the platforms they support.** PIT systems must be designated as such by the responsible OSD or DoD Component heads or their delegates and authorized by an AO specifically appointed to authorize PIT systems.

DoD Facility-Related Control Systems (FRCS)

Categories



Systems

- Building Automation System
- Building Lighting System
- Conveyance/Vertical Transport System
- Electrical Systems
- Heating, Ventilation, Air Conditioning
- Irrigation System
- Shade Control System
- Vehicle Charging System
- Cathodic Protection Systems
- Compressed Air (Or Compressed Gases) System
- Central Plant (District) Chilled Water System
- Central Plant (District) Electrical Power Production
- Central Plant (District) Hot Water System
- Central Plant (District) Steam System
- Electrical Distribution System
- Gray Water System
- Industrial Waste Treatment System
- Microgrid Control Systems
- Natural Gas System
- Oily Water/Waste Oil System
- Potable Water System
- Pure Water System
- Salt Water System
- Sanitary Sewer/Wastewater System
- Utility Metering System (Advanced Meters, AMI, etc.)
- *Many More...*

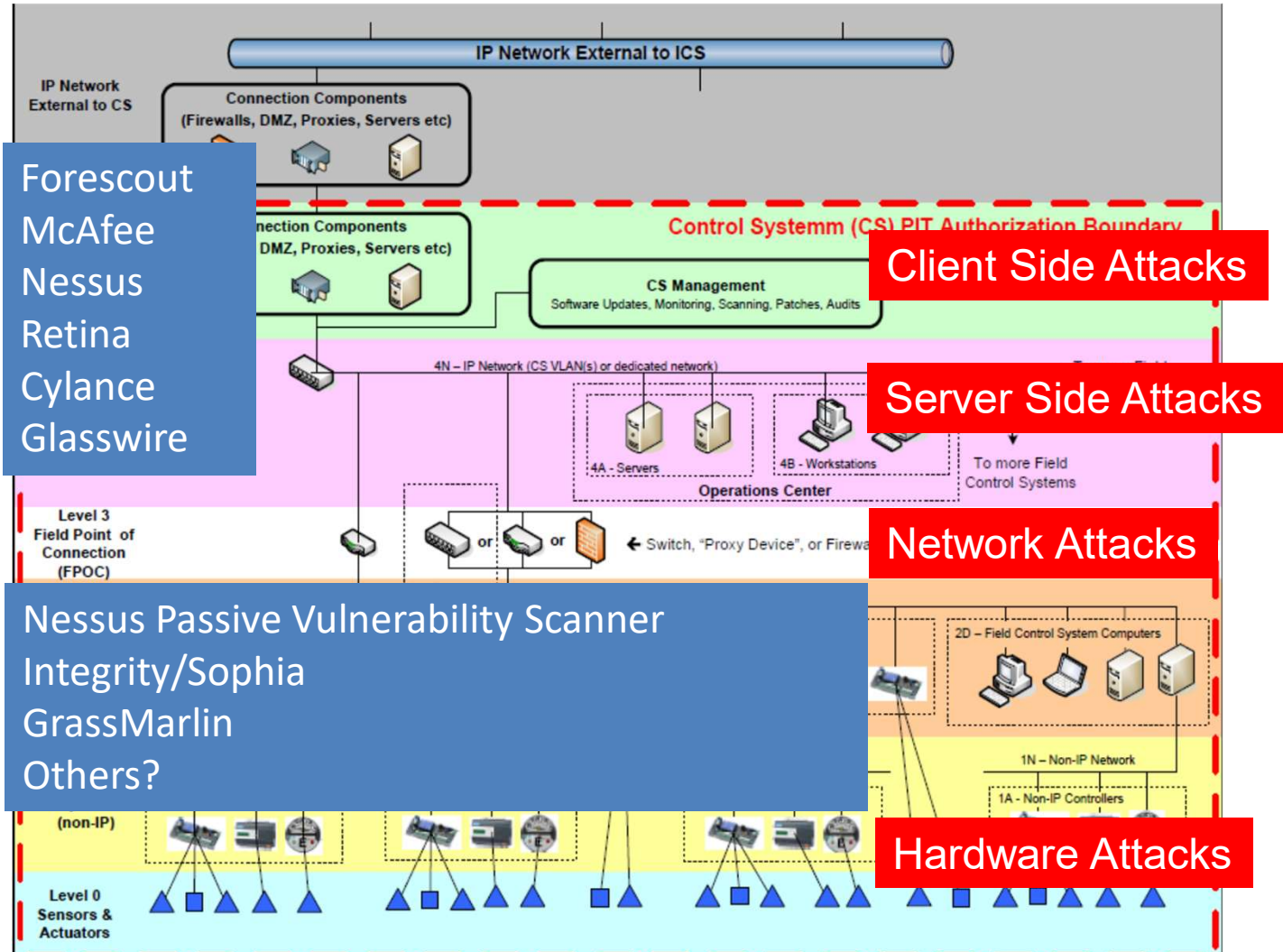
DoD Control Systems are just as vulnerable as industry, how do we protect them?

Continuous Monitoring and Attack Surfaces

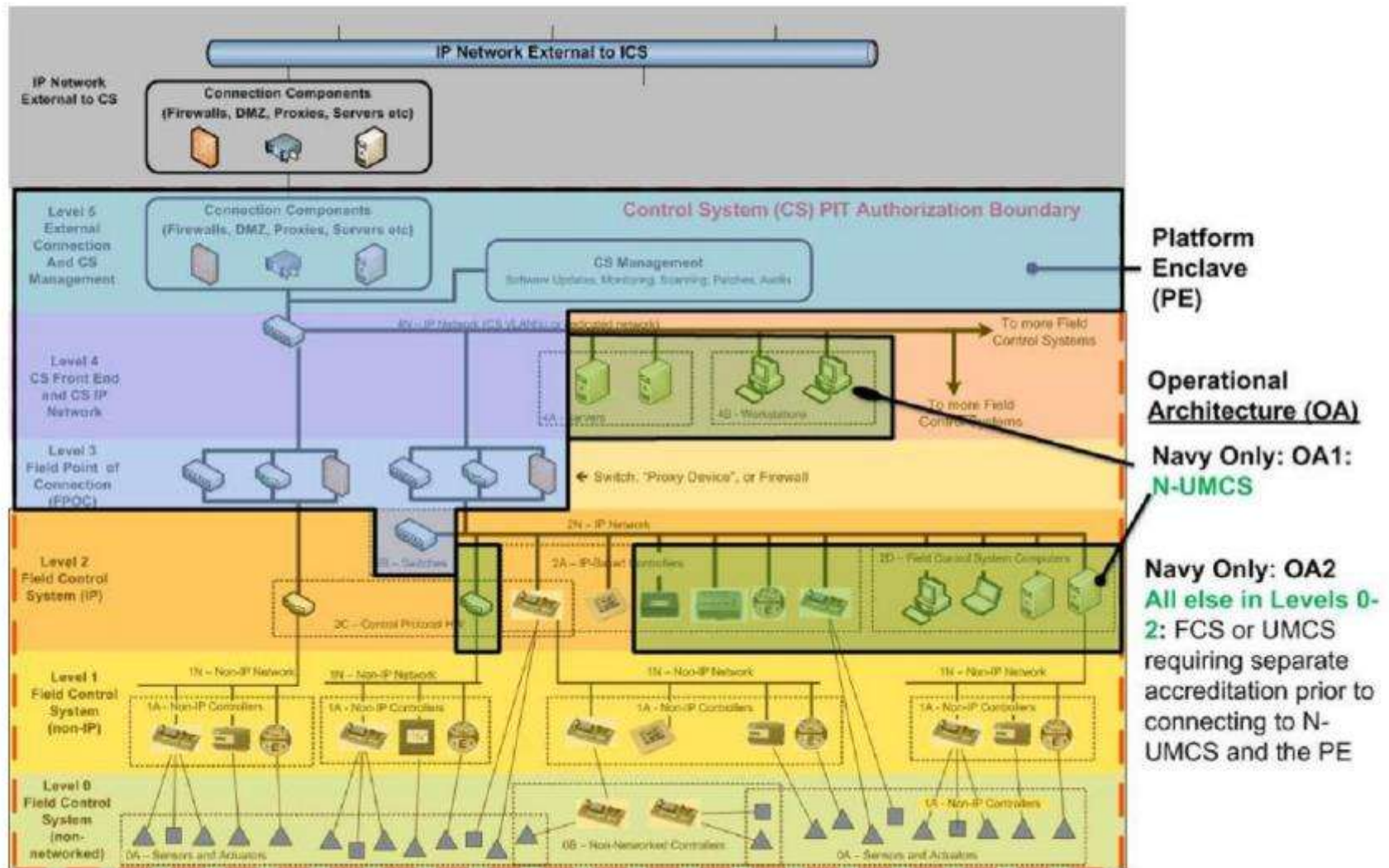
Host Based Security Systems Scanning (Active)

Windows, Linux
HTTP, TCP, UDP

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



DoD UFC 4-010-06 Appendix D



All Control Systems must connect to the Platform Enclave, and must either be separately authorized or fall under the type accreditation of the FRCS-PE and NUMCS.

Personnel IAT II Qualifications

DoDM 8570 – Approved IA Baseline Certifications

<https://public.cyber.mil/cw/cwmp/dod-approved-8570-baseline-certifications/>

As an extension of Appendix 3 to the DoD 8570.01-Manual, the following certifications have been approved as IA baseline certifications for the IA Workforce. Personnel performing IA functions must obtain one of the certifications required for their position category or specialty and level.

Approved Baseline Certifications

IAT Level I	IAT Level II	IAT Level III
A+	CCNA Security	CASP+ CE
CCNA-Security	CySA+ **	CCNP Security
CND	GICSP	CISA
Network+	GSEC	CISSP (or Associate)
SSCP	Security+ CE	GCED
	CND	GCIH
	SSCP	CCSP

Cybersecurity Kickoff Meeting

Agenda

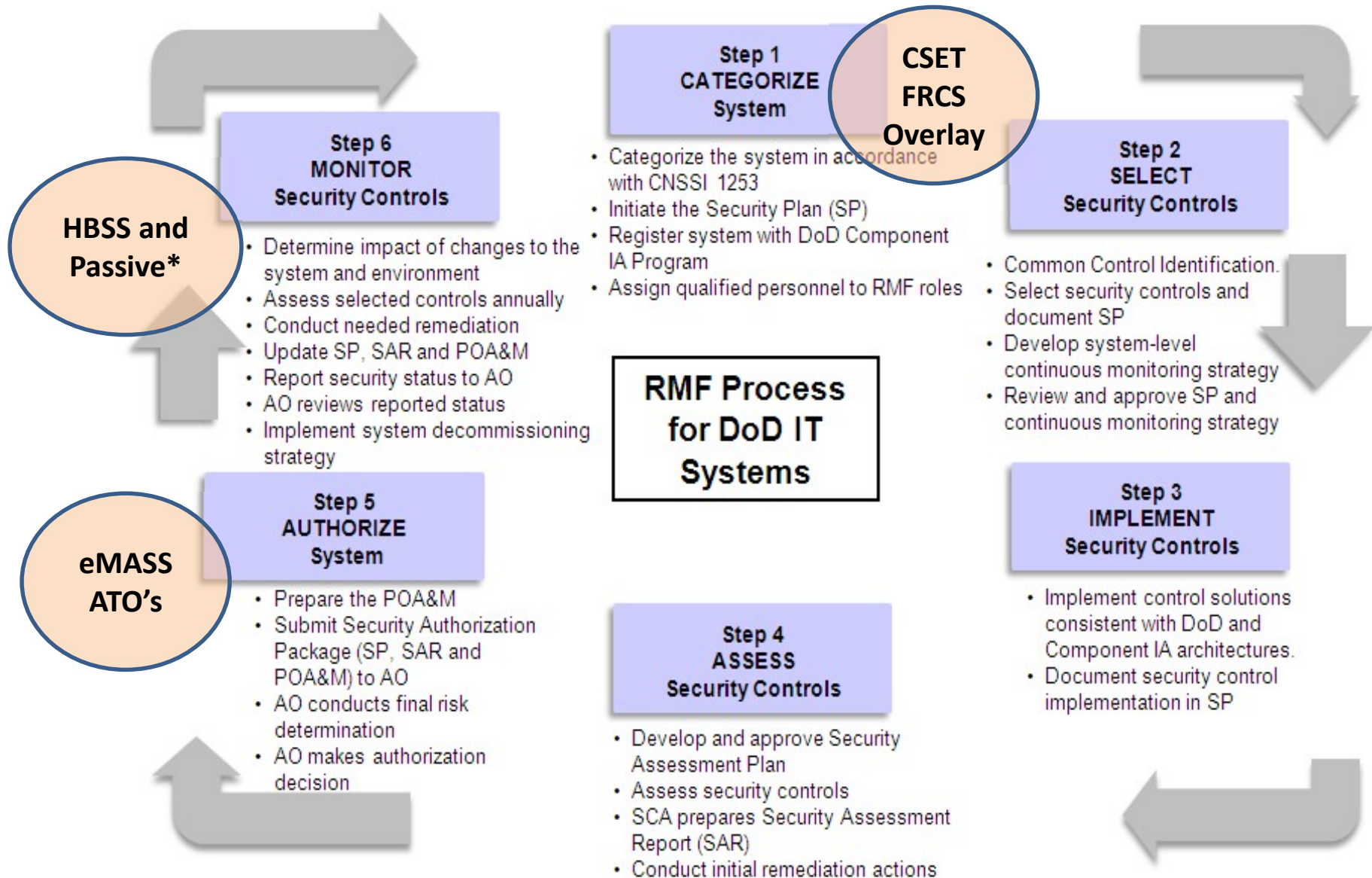
- Stakeholder Introductions (AO, AODR, ISSM, ISSO, ISSE, SO)
- Schedule
- BOQ-A Project Overview
- NAVFAC BOQ-A RFP Cyber Requirements
- Six steps of the RMF – UFGS 25-08-11 Navy RMF
- Define platform enclave /authorization boundary (CRN)
- Initiate eMASS registration – Navy Echelon II Business Rules
- Preliminary Categorization (Navy RMF Steps 1&2)
- Select NIST SP 800-82 security controls
- Create the Authorization Strategy Plan (ASP)
- Develop initial System Security Plan (Excel version)
- Develop ISCP, EICP, EIRP, SAP (artifacts)
- Design construction, Test & Development Environment, FAT & SAT / Commissioning, ISSE Checklist, SCAP Scans, Patch Reports, AV/MW Report, SW Keys and Licenses

UFGS Div 25 Submittals

- ✓ UFGS 25 05 11
 - > SD-01 Pre-Construction
 - > SD-02 Shop Drawings
 - > SD-03 Product Data
 - > SD-06 Test Reports
 - SD-07 Certificates
 - SD-11 Closeout
 - ✓ UFGS 25 08 11.00 20
 - 3.1.1 RMF Step 1 Control System Categorization
 - 3.1.2 RMF Step 2 Security Control Selection
 - 3.1.3 RMF Step 3 Implement Controls
 - 3.1.4 RMF Step 4 Validate Controls
 - > SD-01 Pre-Construction
 - SD-05 Design Data
 - SD-06 Test Reports
 - SD-07 Certificates

ACTIVITY NO	TRANSMITTAL NO	SPEC SECT	DESCRIPTION ITEM SUBMITTED	PARAGRAPH #	CLASSIFICATION	CONTRACTOR SCHEDULE DATES			CONTRACTOR ACTION		
						SUBMIT	APPROVAL NEEDED BY	MATERIAL NEEDED BY	ACCT CODE	DATE OF ACTION	DATE FWD TO APPR AUTH
(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)	(i)	(j)	(k)	(l)
		01 35 13.02	INDUSTRIAL CONTROL SYSTEMS PROCUREMENT								
			SD-03 Product Data								
PCP.SADM-195	0995	1	Network Switches			03/22/22	04/19/22		A	11/06/24	11/06/24
PCP.SADM-200	0995	2	Media Converters			03/15/22	04/07/22		A	11/06/24	11/06/24
PCP.SADM-205	0995	3	Uninterruptible Power Supply (UPS)			03/15/22	04/07/22		A	11/06/24	11/06/24
PCP.SADM-210	0995	4	Remote Terminal Unit (RTU)			03/15/22	04/07/22		A	11/06/24	11/06/24
PCP.SADM-215	0995	5	Intermediary Network Devices			03/15/22	04/07/22		A	11/06/24	11/06/24
			SD-10 Operation and Maintenance Data								
		6	Operator Manual	3.5.1	G	09/07/23	10/04/23				
		7	Sustainment Materials	3.5.2	G	09/07/23	10/04/23				
		8	Security Controls Documents	3.5.3	G	09/07/23	10/04/23				
		9	System Authorization Documents	3.5.3.1	G	09/07/23	10/04/23				
		10	Access Controls Summary	3.5.3.2	G	09/07/23	10/04/23				
		11	Auditing Controls Summary	3.5.3.3	G	09/07/23	10/04/23				
		12	Configuration Management Plan	3.5.3.4	G	09/07/23	10/04/23				
		13	Contingency Plan	3.5.3.5	G	09/07/23	10/04/23				
		14	Security Features Guide	3.5.3.6	G	09/07/23	10/04/23				
		15	Vulnerability Management Plan	3.5.3.7	G	09/07/23	10/04/23				
		16	Maintenance Plan	3.5.3.8	G	09/07/23	10/04/23				
		17	Documented Statements	3.5.3.9	G	09/07/23	10/04/23				
		18	Test Results	3.5.3.10	G	09/07/23	10/04/23				
			SD-11 Closeout Submittals								
		21	Technical Narrative	3.7	G	09/07/23	10/04/23				
		22	Completed Navfac Marianas Ics Checklist	3.6	G	09/07/23	10/04/23				
DIVISION 25 - INTEGRATED AUTOMATION											
		25 05 11	CYBERSECURITY FOR FACILITY - RELATED CONTROL SYSTEMS								
			SD-01 Preconstruction Submittals								
0072		1	Wireless Communication Request	3.1.6.1	G	07/29/22	08/26/22		A	03/09/22	03/29/22
0072		2	Device Account Lock Exception Request	3.1.3.2	G	07/29/22	08/26/22		A	03/09/22	03/29/22
0072		3	Multiple IP Connection Device Request	3.9	G	07/29/22	08/26/22		A	03/09/22	03/29/22
0072		4	Contractor Computer Cybersecurity Compliance	1.9.1.4	G	07/29/22	08/26/22		A	03/09/22	03/29/22

FRCS Overlay & RMF Implementation



Step 1 Categorize the System

<i>USN RMF Information System Categorization Form v1.6</i>				
<i>System Name</i>				
<i>System Acronym</i>				
<i>Version Number</i>				
<i>eMASS Number</i>	<i>Write "N/A" if not registered. For systems registered on SIPR eMASS, write "S-""#</i>			
<i>DITPR ID</i>	<i>Write "N/A" if not registered</i>			
<i>Table 1 - List of RMF Team Members</i>			<i>Table 2 - Additional Considerations</i>	
<i>The personnel listed in the table below are the RMF team members associated with the system being categorized. Additional personnel can be added as required, including Information Owner (IO), joint AO, or others.</i>			<i>In the table below, select the answer from each drop-down list that applies to your system for each question.</i>	
Role	Name	Organization	<i>Classification of System</i>	
<i>PM</i>			<i>Classification of Information</i>	
<i>ISO (if different)</i>			<i>Releasability of Information</i>	
<i>ISSM</i>			<i>Applicable Required Overlays</i>	
<i>User Representative</i>			<i>Any Interconnected Systems/External Services which could elevate impact level?</i>	

Step 2 Select Controls (eMASS)

Exported on 25-Sep-2023 by MICHAEL CHIPLEY

Control / AP Information (read-only)							Latest Test Results (read-only)		
Implemented	Hybrid	-	CP-2.1	000443	000443: The organization develops a contingency plan for the information system that identifies essential missions.	<p>The organization being inspected/assessed must clearly and accurately document essential missions for its information system(s). Impact of loss of essential mission functions must be defined using CNSSI 1253.</p> <p>Recommended Compelling Evidence: 1) Signed and dated contingency plan, referencing essential missions section</p>	<p>The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents essential missions for its information system(s).</p>	Local	<p>Reference the NLCN BCS Contingency Plan with the essential missions section.</p> <p>Compelling Evidence: 1) Signed and dated contingency plan, referencing essential missions section</p>

Step 3 Implement Controls

Cyber Risk Management Plan
System Security Plan (SSP) [COMPANY LOGO]

TABLE OF CONTENTS

1. INTRODUCTION	6
2. SYSTEM IDENTIFICATION	6
3. SYSTEM ENVIRONMENT	6
3.1 NETWORK DIAGRAMS	6
3.1.1 NETWORK ARCHITECTURE	6
3.1.2 [Application Name] BACKUP	7
3.1.3 CENTRALIZED LOG COLLECTOR AND ANALYZER	7
3.2 INVENTORY LIST	7
4. ROLES AND RESPONSIBILITIES	9
4.1 EXECUTIVE MANAGEMENT	9
4.2 CHIEF SECURITY OFFICER (CSO) OR CHIEF INFORMATION SECURITY OFFICER (CISO)	9
4.3 SECURITY STEERING COMMITTEE/CONFIGURATION CONTROL BOARD	10
4.4 DATA OWNERS	10
4.5 SECURITY ADMINISTRATORS	10
4.6 SUPERVISORS/MANAGERS	10
4.7 USERS	11
5. RISK ANALYSIS	11
6. IMPACT LEVELS, INFORMATION AND DATA TYPES	11
6.1 BASIC MODEL	11
6.1.1 CONFIDENTIALITY	11
6.1.2 INTEGRITY	12
6.1.3 AVAILABILITY	12
6.2 SECURITY ASSURANCE LEVEL (SAL)	12
6.3 DHS CSET TOOL FIPS 199 SECURITY ASSURANCE LEVEL GUIDANCE	13
7. SECURITY CONTROLS	14

Controlled Unclassified Information (CUI)
System Security Plan (SSP)

Step 3 Implement Controls

ORG
CORPORATE RISK MANAGEMENT PLAN
SECURITY MONTHLY AUDIT REPORT (SMAR)
CONFIGURATION BASELINE

December 30, 2020

CLIENT

Controlled Unclassified Information (CUI)

Corporate Risk Management Plan
Security Monthly Audit Report (SMAR)

TABLE OF CONTENTS

1. INTRODUCTION AND PURPOSE	7
2. WORK SITES AND GENERAL SYSTEM DESCRIPTION	8
3. DECEMBER 2020 AUDIT INFORMATION	11
3.1 SYSTEM ADMIN LOGIN VERIFICATION	11
3.2 MICROSOFT SERVER 2019 (ORFP-BASIC1)	11
3.2.1 WINDOWS SERVER 2019 – CONTROL PANEL SYSTEM INFORMATION (ORFP-BASIC1)	12
3.2.2 WINDOWS SERVER 2019 – CONTROL PANEL USER ACCOUNTS	12
3.2.3 WINDOWS SERVER 2019 – SERVER MANAGER DASHBOARD	13
3.2.4 WINDOWS SERVER 2019 – SERVER MANAGER LOCAL SERVER PROPERTIES (ORFP-BASIC1) LAST INSTALLED UPDATES 6/5/2018.....	13
3.2.5 WINDOWS SERVER 2019 – SERVER MANAGER SYSTEM INFORMATION SYSTEM SUMMARY (ORFP- BASIC1)	14
3.2.6 WINDOWS SERVER 2019 – SYSTEM INFORMATION SOFTWARE ENVIRONMENT	14
3.2.7 WINDOWS SERVER 2019 – SYSTEM INFORMATION BITLOCKER (NOT ENABLED)	15
3.2.8 WINDOWS SERVER 2019 – CONTROL PANEL DEVICES AND PRINTERS	15
3.2.9 WINDOWS SERVER 2019 – FIREWALL WITH ADVANCED SECURITY MONITORING	16
3.2.10 WINDOWS SERVER 2019 – CONTROL PANEL SECURITY AND MAINTENANCE	16
3.2.11 WINDOWS SERVER 2019 – CONTROL PANEL INTERNET PROPERTIES (TLS 1.0 AND 1.1 ENABLED)	17
3.2.12 WINDOWS SERVER 2019 – CONTROL PANEL INTERNET PROPERTIES (TLS 1.0 and 1.1 DISABLED, 1.2 ENABLED) 17	17
3.2.13 WINDOWS SERVER 2019 – CONTROL PANEL WINDOWS FIREWALL (ON).....	18
3.2.14 WINDOWS SERVER 2019 – WINDOWS FIREWALL WITH ADVANCED SECURITY INBOUND RULES 1	18
3.2.15 WINDOWS SERVER 2019 – WINDOWS FIREWALL WITH ADVANCED SECURITY INBOUND RULES 2	19
3.2.16 WINDOWS SERVER 2019 – WINDOWS FIREWALL WITH ADVANCED SECURITY INBOUND RULES 3	19
3.2.17 WINDOWS SERVER 2019 – WINDOWS FIREWALL WITH ADVANCED SECURITY INBOUND RULES 4	20
3.2.18 WINDOWS SERVER 2019 – WINDOWS FIREWALL WITH ADVANCED SECURITY INBOUND RULES 5	20
3.2.19 WINDOWS SERVER 2019 – WINDOWS FIREWALL WITH ADVANCED SECURITY INBOUND RULES 6	21
3.2.20 WINDOWS SERVER 2019 – WINDOWS FIREWALL WITH ADVANCED SECURITY OUTBOUND RULES 1 21	21
3.2.21 WINDOWS SERVER 2019 – WINDOWS FIREWALL WITH ADVANCED SECURITY OUTBOUND RULES 2 22	22
3.2.22 WINDOWS SERVER 2019 – WINDOWS FIREWALL WITH ADVANCED SECURITY OUTBOUND RULES 3 22	22
3.2.23 WINDOWS SERVER 2019 – WINDOWS FIREWALL WITH ADVANCED SECURITY OUTBOUND RULES 4 23	23
3.2.24 WINDOWS SERVER 2019 – CONTROL PANEL PROGRAMS AND FEATURES 1	23
3.2.25 WINDOWS SERVER 2019 – CONTROL PANEL PROGRAMS AND FEATURES 2	24
3.2.26 WINDOWS SERVER 2019 – CONTROL PANEL PROGRAMS AND FEATURES INSTALLED UPDATES 1	24
3.2.27 WINDOWS SERVER 2019 – CONTROL PANEL PROGRAMS AND FEATURES INSTALLED UPDATES 2	25

Controlled Unclassified Information
Security Monthly Audit Report (SMAR)

Configuration Baseline Audit Report

3.3.1.12	JCI METASYS 12 DELL LATTITUDE LAPTOP – DEVICE PERFORMANCE & HEALTH (NO ISSUES)...	45
3.3.1.13	JCI METASYS 12 DELL LATTITUDE LAPTOP – FAMILY OPTIONS (DISABLED)	46
3.3.1.14	JCI METASYS 12 DELL LATTITUDE LAPTOP – PROTECTION HISTORY (NO ACTIONS)	46
3.3.1.15	JCI METASYS 12 DELL LATTITUDE LAPTOP – DEVICES & PRINTERS	47
3.3.1.16	JCI METASYS 12 DELL LATTITUDE LAPTOP – CONTROL PANEL REMOTEAPPS AND DESKTOP CONNECTION (DISABLED)	48
3.3.1.17	JCI METASYS 12 DELL LATTITUDE LAPTOP – DISK MANAGEMENT (HEALTHY).....	48
3.3.1.18	JCI METASYS 12 DELL LATTITUDE LAPTOP – WINDOWS APPLICATION LOG	49
3.3.1.19	JCI METASYS 12 DELL LATTITUDE LAPTOP – WINDOWS SECURITY LOG	50
3.3.1.20	JCI METASYS 12 DELL LATTITUDE LAPTOP – WINDOWS SYSTEM LOG.....	51
3.3.1.21	JCI METASYS 12 DELL LATTITUDE LAPTOP – DESKTOP	52
3.3.1.22	JCI METASYS 12 DELL LATTITUDE LAPTOP – SCAP SCAN 1 (INITIAL).....	53
3.3.1.23	JCI METASYS 12 DELL LATTITUDE LAPTOP – SCAP SCAN 2 (FINAL)	53
3.3.2	BUILDING CONTROL SYSTEM, HVAC – JCI METASYS, YORK SPLIT SYSTEM, GFORCE CRAC UNIT.....	54
3.3.3	BUILDING CONTROL SYSTEM, LIGHTING – COLUMBIA LIGHTING	56
3.3.4	FIRE LIFE SAFETY AND MASS NOTIFICATION – KINGFISHER/FEDERAL SIGNAL	58
3.3.5	UTILITY CONTROL SYSTEM – ELECTRICAL DISTRIBUTION	60
3.3.6	UTILITY METERING SYSTEM – AMI ELECTRICAL AND WATER – SCHNEIDER ION 8560/TBD.....	61

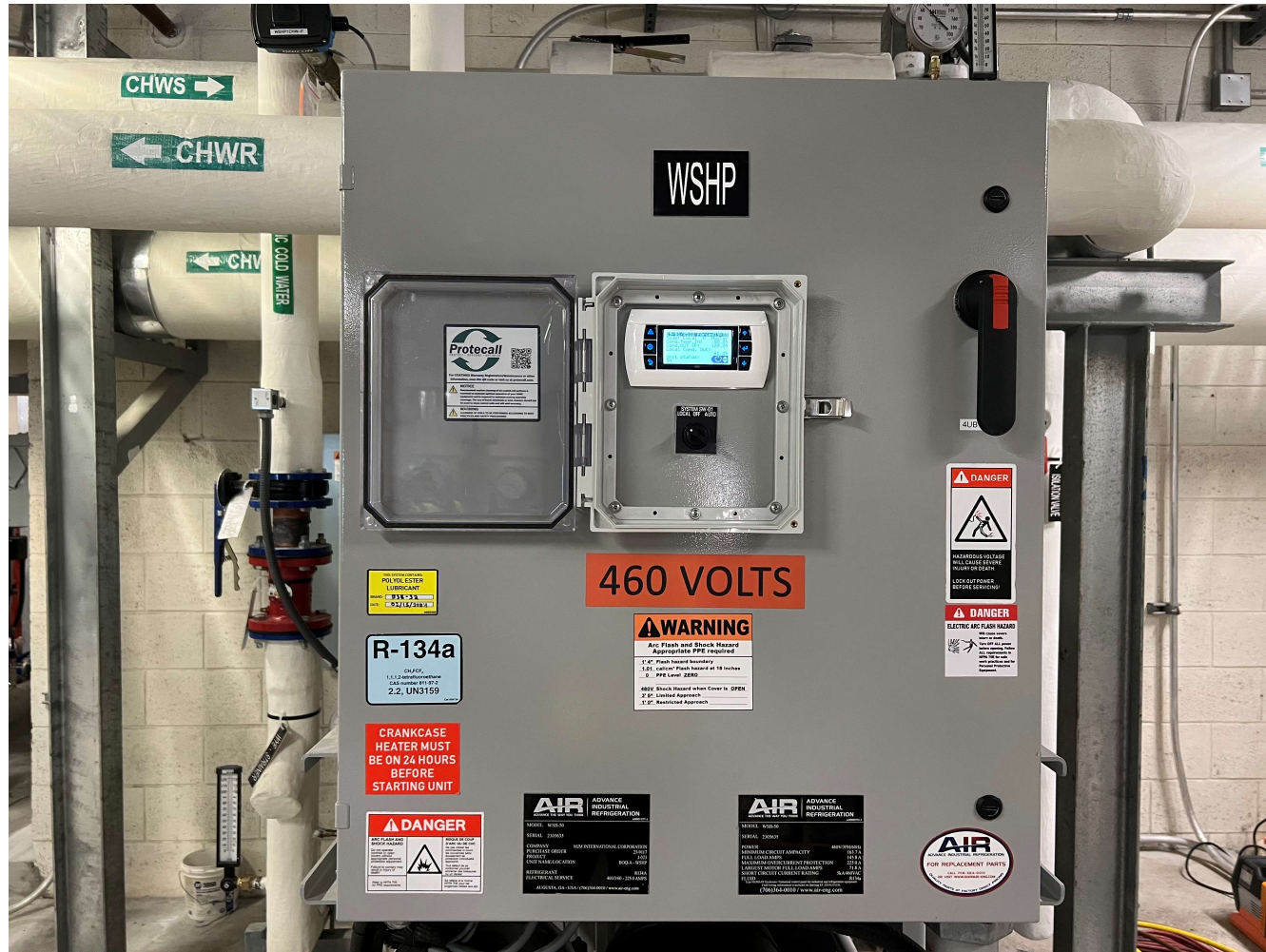
Typical Site Photos of FRCS



Typical Site Photos of FRCS



Typical Site Photos of FRCS



Typical Site Photos of FRCS



Typical Site Photos of FRCS



Typical Site Photos of FRCS



Typical Site Photos of FRCS



Typical Site Photos of FRCS



Typical Site Photos of FRCS



Typical Site Photos of FRCS



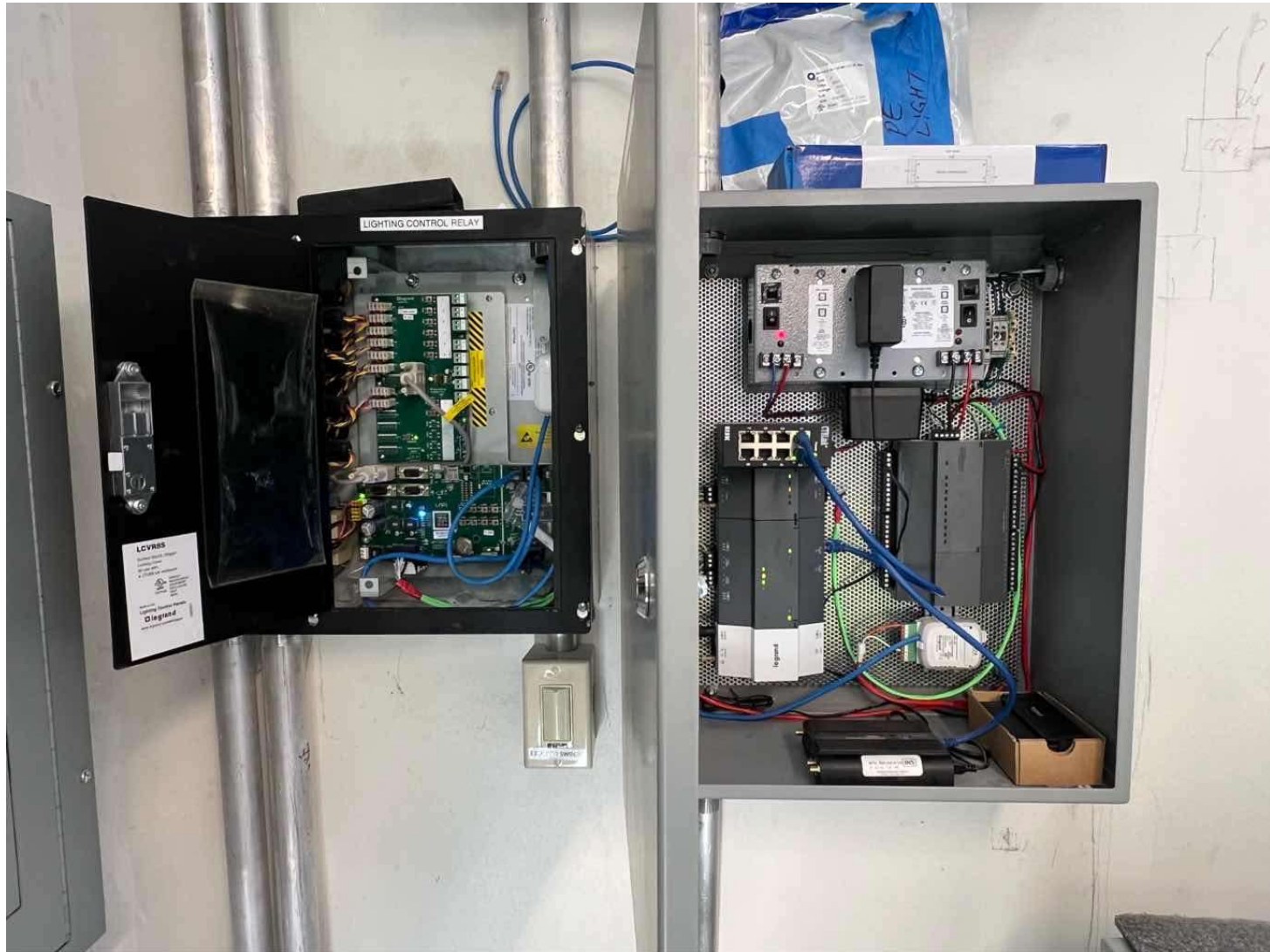
Typical Site Photos of FRCS



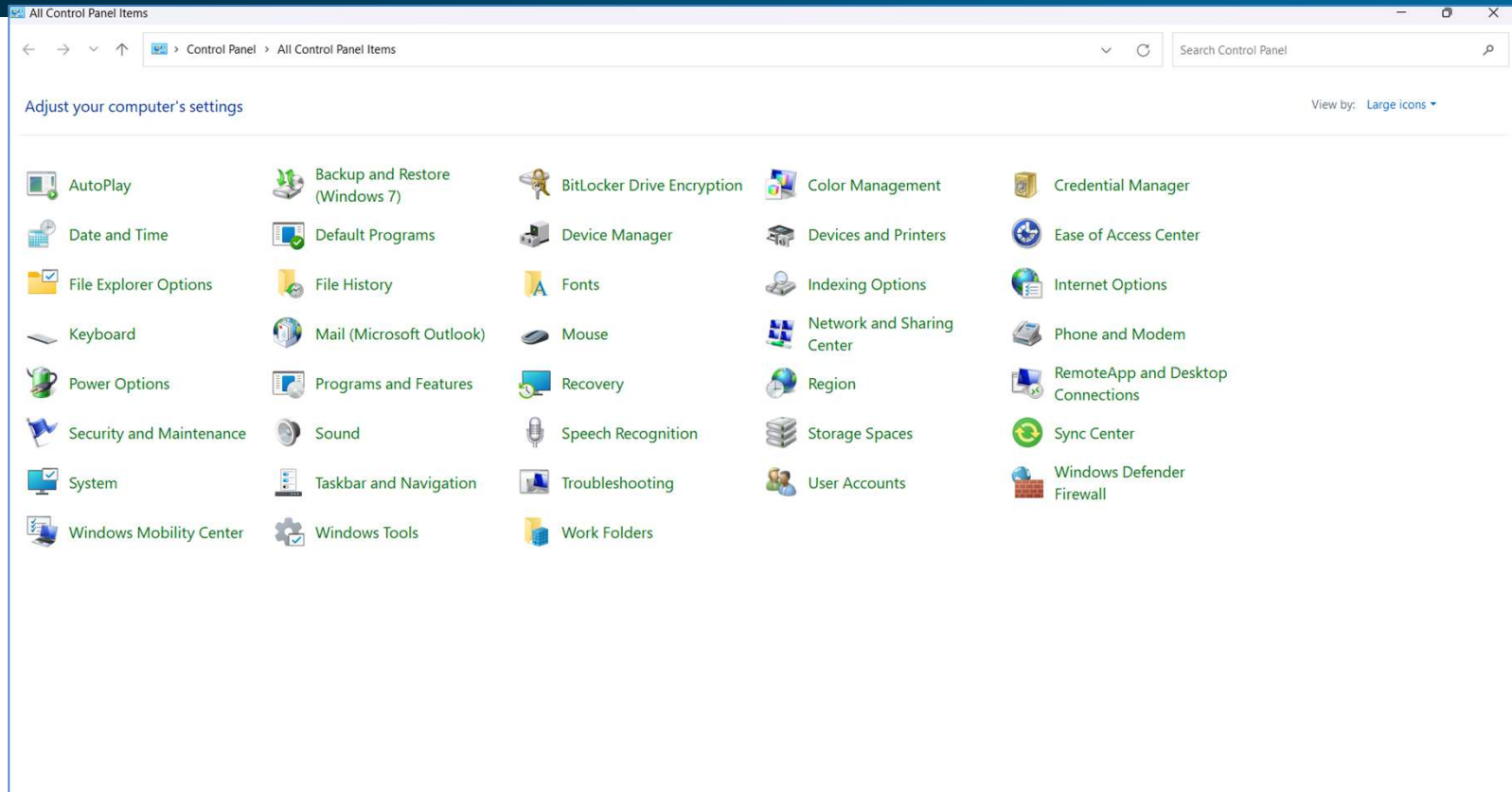
Typical Site Photos of FRCS



Typical Site Photos of FRCS



Control Panel



The Control Panel can access 90% of key settings and operations:

- BitLocker Full Disk Encryption Data at Rest
- Transport Layer Settings 1.2 and 1.3 Data Encryption in Transit (web pages)
- Windows Defender Firewall
- Security and Maintenance
- Backup and Retore
- User Accounts

BitLocker On

The image shows a Windows desktop environment. On the left, the BitLocker Drive Encryption control panel window is open, displaying the status of the operating system drive (C:) as 'BitLocker on' and a removable drive (My Passport (E:)) as 'BitLocker off'. The control panel window includes options such as 'Suspend protection', 'Back up your recovery key', 'Change password', 'Remove password', and 'Turn off BitLocker'. On the right, the desktop background features a night sky with the Milky Way and a green tent in the foreground. A system information window is overlaid on the bottom right of the desktop, providing details about the host name, boot time, CPU, free space, machine domain, memory, OS, service pack, snapshot time, system type, volumes, and user name.

BitLocker Drive Encryption
Control Panel Home

BitLocker Drive Encryption
Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

Operating system drive

C: BitLocker on

- Suspend protection
- Back up your recovery key
- Change password
- Remove password
- Turn off BitLocker

Fixed data drives

Removable data drives - BitLocker To Go

My Passport (E:) BitLocker off

See also

- TPM Administration
- Disk Management
- Privacy statement

Host Name: CCS-HISTORIAN

Boot Time: 6/26/2024 11:30 AM
CPU: 16 Core 3.40 GHz Intel Xeon(R) W-1270
Free Space: C: 13561.90 GB NTFS
Machine Domain: WORKGROUP
Memory: 32446 MB
OS: Windows Server 2019 Standard
Service Pack: No service pack
Snapshot Time: 6/26/2024 11:34 AM
System Type: Server, Stand-alone, Terminal Server
Volumes: C: 13722.65 GB NTFS
User Name: Array

12:35 PM
6/26/2024

Internet Options Advanced - TLS 1.2 Enabled

The screenshot shows the Windows Internet Properties dialog box, specifically the Advanced tab. The 'Settings' section is expanded, and the following options are checked:

- Enable 64-bit processes for Enhanced Protected Mode*
- Enable DOM Storage
- Enable Enhanced Protected Mode*
- Enable Integrated Windows Authentication*
- Enable native XMLHttpRequest support
- Enable Windows Defender SmartScreen
- Send Do Not Track requests to sites you visit in Internet E
- Use SSL 3.0
- Use TLS 1.0
- Use TLS 1.1
- Use TLS 1.2
- Warn about certificate address mismatch*
- Warn if changing between secure and not secure mode
- Warn if POST submittal is redirected to a zone that does n

Below the settings, there is a 'Restore advanced settings' button and a 'Reset Internet Explorer settings' section with a 'Reset...' button. A yellow information bar at the bottom of the dialog states: 'Some settings are managed by your system administrator.'

The desktop background features a night landscape with a tent and mountains. In the bottom right corner, system information is displayed:

Host Name: CCS-HISTORIAN
Boot Time: 6/26/2024 11:30 AM
CPU: 16 Core 3.40 GHz Intel Xeon(R) W-1270
Free Space: C:\ 3561.90 GB NTFS
Machine Domain: WORKGROUP
Memory: 32446 MB
OS : Windows Server 2019 Standard
Service Pack: No service pack
Snapshot Time: 6/26/2024 11:34 AM
System Type: Server, Stand-alone, Terminal Server
Volumes: C:\ 3722.65 GB NTFS
User Name: Array

The system tray in the bottom right corner shows the time as 1:03 PM on 6/26/2024.

Windows Firewall - On

The image shows a Windows Security window titled "Windows Security" with the "Firewall & network protection" settings open. The settings are for a "Public network (active)" and show that the firewall is on. The left sidebar lists other security features like "Virus & threat protection", "App & browser control", and "Device security". The right sidebar contains links for "Windows Community videos", "Who's protecting me?", and "Change your privacy settings".

Windows Security

Firewall & network protection

Who and what can access your networks.

- Domain network**
Firewall is on.
- Private network**
Firewall is on.
- Public network (active)**
Firewall is on.

[Allow an app through firewall](#)
[Network and Internet troubleshooter](#)
[Firewall notification settings](#)
[Advanced settings](#)
[Restore firewalls to default](#)

Windows Community videos
[Learn more about Firewall & network protection](#)

Who's protecting me?
[Manage providers](#)

Change your privacy settings
View and change privacy settings for your Windows 10 device.
[Privacy settings](#)
[Privacy dashboard](#)
[Privacy Statement](#)

Host Name: CCS-HISTORIAN
Boot Time: 6/26/2024 11:30 AM
CPU: 16 Core 3.40 GHz Intel Xeon(R) W-1270
Free Space: C:\ 3561.90 GB NTFS
Machine Domain: WORKGROUP
Memory: 32446 MB
OS: Windows Server 2019 Standard
Service Pack: No service pack
Snapshot Time: 6/26/2024 11:34 AM
System Type: Server, Stand-alone, Terminal Server
Volumes: C:\ 3722.65 GB NTFS
User Name: Array

2023-04 - Engine 2...
NLON-CH...

1:11 PM
6/26/2024

Windows Security AV Scan – No Threats

The screenshot displays the Windows Security application window. The 'Threat history' section shows a successful scan on 6/26/2024 at 3:37 AM, with 0 threats found. The system information panel on the right provides details about the host, including the name 'CCS-HISTORIAN', CPU, memory, and OS.

Windows Security

Threat history

View detected threats and scan details.

Last scan

Windows Defender Antivirus automatically scans your device for viruses and other threats to help keep it safe.

Last scan: 6/26/2024 3:37 AM (quick scan)
0 threats found.
Scan lasted 30 seconds
13913 files scanned.

Quarantined threats

Quarantined threats have been isolated and prevented from running on your device. They will be periodically removed.

No threats.

Allowed threats

Allowed threats are items identified as threats, which you allowed to run on your device.

No threats.

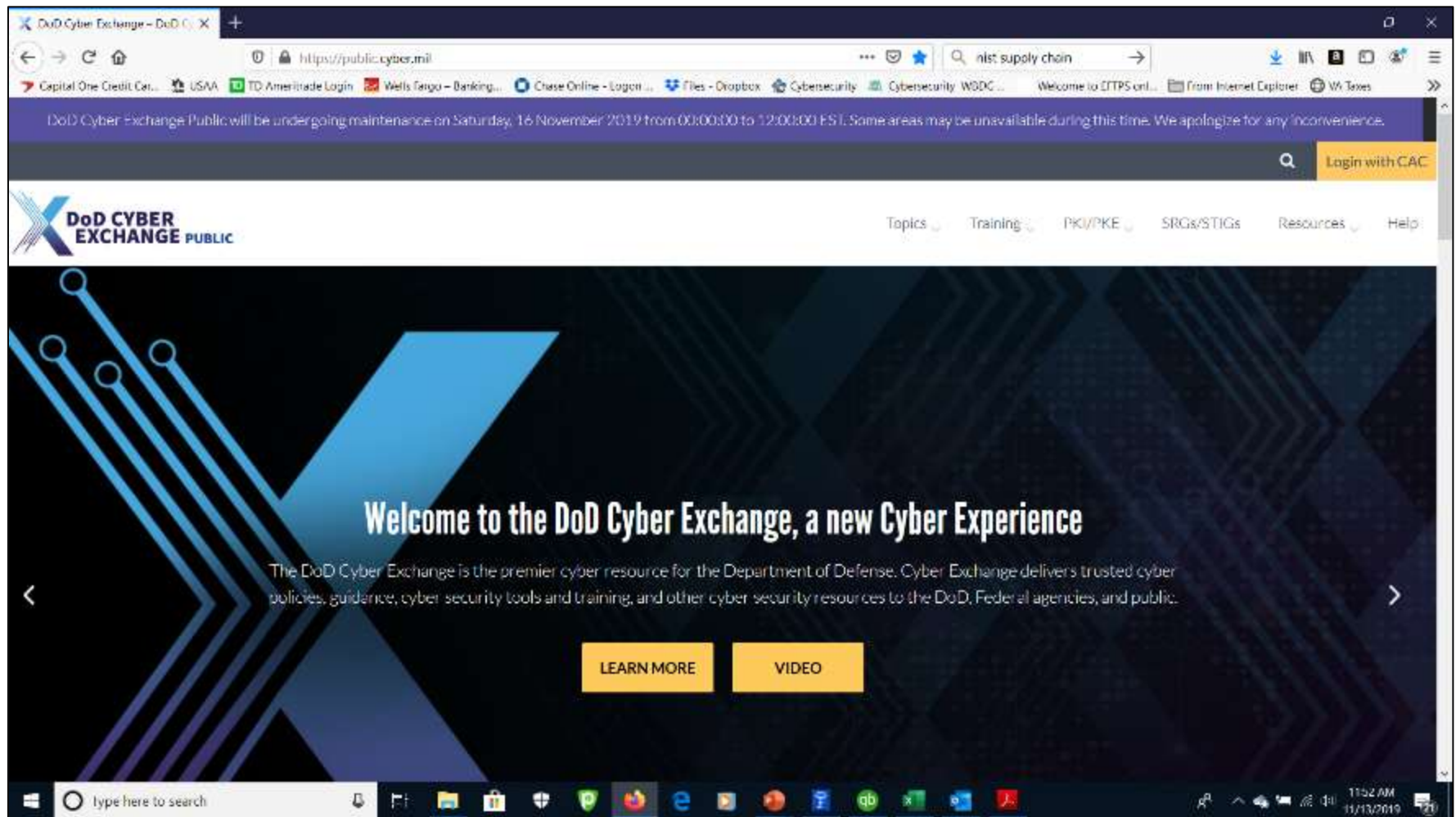
[See full history](#)

[Change your privacy settings](#)
View and change privacy settings for your Windows 10 device.
[Privacy settings](#)
[Privacy dashboard](#)
[Privacy Statement](#)

Host Name: CCS-HISTORIAN
Boot Time: 6/26/2024 11:30 AM
CPU: 16 Core 3.40 GHz Intel Xeon(R) W-1270
Free Space: C:\ 3561.90 GB NTFS
Machine Domain: WORKGROUP
Memory: 32446 MB
OS: Windows Server 2019 Standard
Service Pack: No service pack
Snapshot Time: 6/26/2024 11:34 AM
System Type: Server, Stand-alone, Terminal Server
Volumes: C:\ 3722.65 GB NTFS
User Name: Array

Taskbar: 1:46 PM 6/26/2024

DISA STIGs



<https://public.cyber.mil/>

DISA STIGs

Sessions: 10 Files: 361 Total Size (MB): 111.34

Filter by session, hostname or content.

Scan Session	Status	Directory	Files	Size (MB)	Hosts	Content	Errors	Warnings	Ave %	Max %	Min %
2022-02-22_234521		C:\Users\Administrator\SCC\Sessions\2022-02-22_234521\	36	10.36	1	6	0	0	98.4	95.26	100
2022-02-22_234120		C:\Users\Administrator\SCC\Sessions\2022-02-22_234120\	36	10.36	1	6	0	0	95.06	95.26	100
2022-02-22_233531		C:\Users\Administrator\SCC\Sessions\2022-02-22_233531\	36	10.36	1	6	0	0	95.06	95.26	100
2022-02-22_230734		C:\Users\Administrator\SCC\Sessions\2022-02-22_230734\	36	10.54	1	6	0	0	78.48	95.73	0
2022-02-22_225943		C:\Users\Administrator\SCC\Sessions\2022-02-22_225943\	36	10.74	1	6	0	0	76.5	95.12	0
2022-02-22_163034		C:\Users\Administrator\SCC\Sessions\2022-02-22_163034\	37	11.49	1	6	63	0	52.6	84.36	0
2022-02-22_162436	* new *	C:\Users\Administrator\SCC\Sessions\2022-02-22_162436\	36	11.69	1	6	0	0	49.32	80	0
2022-02-22_161414	* new *	C:\Users\Administrator\SCC\Sessions\2022-02-22_161414\	36	11.69	1	6	0	0	49.4	80	0
2022-02-22_160626	* new *	C:\Users\Administrator\SCC\Sessions\2022-02-22_160626\	36	11.94	1	6	0	0	39.38	80	0
2022-02-21_234247	* new *	C:\Users\Administrator\SCC\Sessions\2022-02-21_234247\	36	12.17	1	6	0	0	31.22	80	0

Host Name	Content	Score	Errors	Warnings
CCS-STATION1	Windows_Firewall_Advanced_Security	100	0	0
CCS-STATION1	Windows_Defender_Antivirus	95.12	0	0
CCS-STATION1	Windows_10_STIG	95.26	0	0
CCS-STATION1	MS_Edge_STIG	100	0	0
CCS-STATION1	MS_Dot_Net_Framework	100	0	0
CCS-STATION1	IE_11_STIG	100	0	0

Report Type	Format	Filename	Size (MB)
All Settings	HTML	Results/SCAP/CCS-STATION1_SCC-5.4.2_2022-02-22_ws_Firewall_with_Advanced_Security-002.001.html	0.31
Non-Compliance	HTML	Results/SCAP/CCS-STATION1_SCC-5.4.2_2022-02-22_ws_Firewall_with_Advanced_Security-002.001.html	0.01

The STIGs contain technical guidance to "lock down" information systems/software that might otherwise be vulnerable to a malicious computer attack. We want scores of 90 or better.

Computer Management Disk

The screenshot displays the Windows Computer Management console, specifically the Disk Management section. The main area shows a table of disk volumes with the following data:

Volume	Layout	Type	File System	Status	Capacity	Free Space	% Free
(Disk 0 partition 1)	Simple	Basic		Healthy (EFI System Partition)	300 MB	300 MB	100 %
(Disk 0 partition 4)	Simple	Basic		Healthy (Recovery Partition)	900 MB	900 MB	100 %
(Disk 0 partition 5)	Simple	Basic		Healthy (Recovery Partition)	19.93 GB	19.93 GB	100 %
Windows (C:)	Simple	Basic	NTFS (BitLocker Encrypted)	Healthy (Boot, Page File, Crash Dump, Basic Data Partition)	932.64 GB	119.26 GB	13 %

Below the table, a graphical representation of Disk 0 is shown. It is a Basic disk with a total capacity of 953.74 GB and is Online. The disk layout includes:

- 300 MB Healthy (EFI System Partitio)
- 932.64 GB NTFS (BitLocker Encrypted) Healthy (Boot, Page File, Crash Dump, Basic Data Partition)
- 900 MB Healthy (Recovery Partition)
- 19.93 GB Healthy (Recovery Partition)

A legend at the bottom indicates that black represents Unallocated space and blue represents Primary partition.

Disk Healthy and Plenty of Disk Space

Computer Management Event Logs

The screenshot shows the Windows Event Viewer interface. The left pane displays the navigation tree with 'Application' logs selected. The main pane shows a filtered list of events with the following columns: Level, Date and Time, Source, Event ID, and Task Category. The right pane shows the 'Actions' menu with options like 'Open Saved Log...', 'Create Custom View...', and 'Event Properties'.

Level	Date and Time	Source	Event ID	Task Category
Warning	8/27/2024 12:24:09 PM	RestartManager	10010	None
Warning	8/27/2024 12:24:09 PM	RestartManager	10010	None
Warning	8/27/2024 12:24:09 PM	RestartManager	10010	None
Warning	8/27/2024 12:24:09 PM	RestartManager	10010	None
Warning	8/27/2024 12:24:09 PM	RestartManager	10010	None
Warning	8/27/2024 12:29:17 PM	RestartManager	10010	None
Warning	8/27/2024 1:25:51 PM	Search	10024	Gatherer
Warning	8/27/2024 1:25:51 PM	Search	10024	Gatherer
Warning	8/27/2024 12:29:18 PM	RestartManager	10010	None
Warning	8/27/2024 12:29:18 PM	RestartManager	10010	None
Warning	8/27/2024 12:29:18 PM	RestartManager	10010	None
Warning	8/27/2024 12:29:18 PM	RestartManager	10010	None
Warning	8/27/2024 10:13:13 AM	RestartManager	10010	None
Warning	8/27/2024 9:48:05 AM	RestartManager	10010	None
Warning	8/27/2024 9:48:05 AM	RestartManager	10010	None
Warning	8/27/2024 9:48:05 AM	RestartManager	10010	None
Warning	8/27/2024 9:48:05 AM	RestartManager	10010	None
Warning	7/24/2024 4:21:00 PM	WMI	63	None
Warning	7/24/2024 1:29:48 AM	Search	10024	Gatherer
Warning	8/27/2024 9:48:05 AM	RestartManager	10010	None
Warning	8/27/2024 10:13:13 AM	RestartManager	10010	None
Warning	8/27/2024 10:13:13 AM	RestartManager	10010	None
Warning	8/27/2024 10:13:13 AM	RestartManager	10010	None

Event 10010, RestartManager

General Details

Application 'C:\Program Files\Microsoft Office\root\vfs\ProgramFilesCommonX64\Microsoft Shared\OFFICE16\ai.exe' (pid 22560) cannot be restarted - Application SID does not match Conductor SID.

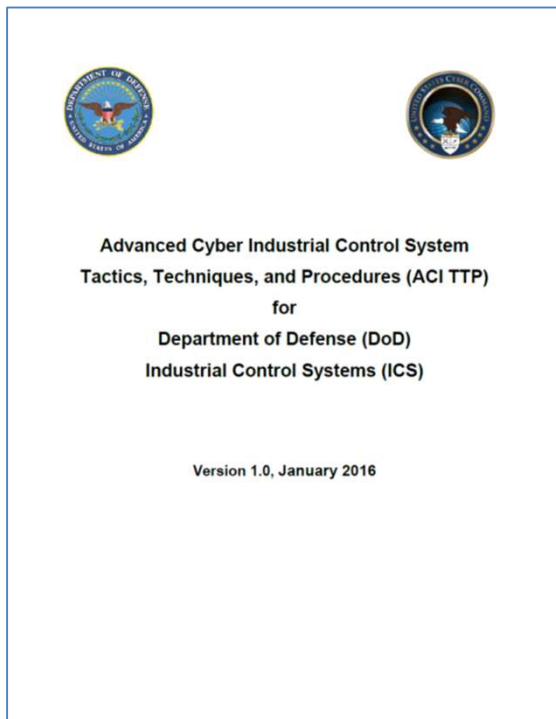
Log Name: Application
Source: RestartManager
Event ID: 10010
Level: Warning
User: SYSTEM

Logged: 8/27/2024 12:29:18 PM
Task Category: None
Keywords:
Computer: LT13-Mike

Check for Critical, Warning and Error, research the Event ID's to resolve

ACI TTP for DoD ICS

The scope of the ACI TTP includes all DoD ICS. DoD ICS, which include **supervisory control and data acquisition (SCADA) systems, distributed control systems (DFRCS)**, and other control system configurations, such as skid-mounted programmable logic controllers (PLC) are typical configurations found throughout the DoD. **ICS are often used in the DoD to manage sectors of critical infrastructure such as electricity, water, wastewater, oil and natural gas, and transportation.**



3. How to Use These TTP

This ACI TTP is divided into essentially four sections:

- **ACI TTP Concepts** (chapters 2 through 4)
- **Threat-Response Procedures (Detection, Mitigation, Recovery)** (enclosures A, B, and C)
- **Routine Monitoring of the Network and Baselining the Network** (enclosures D and E)
- **Reference Materials** (enclosures F through I and appendix A through D)

TTP 's Apply to IT and OT

The Tactics, Techniques and Procedures can be used by any organization and apply to:

Information Technology (IT) Systems – Business and Home

Operational Technologies (OT) Systems – Any Kind (Utility, Building, Environmental, Medical, Logistics, Transportation, Weapons, etc.)

The tools that will be used are almost all open source and free to use (premium or business versions are modestly priced)

- ***Segment and VLAN IT and OT networks; DMZ's with gateways and/or firewalls***
- ***Separate the OS and OT data (C: OS and D: OT data), enable BitLocker on both drives***

Key Roles

AO-Authorizing Official NAVFAV HQ

SO-System Owner NAVFAV Public Works Directorate

ISSM-Information System Security Manager CIO2 and 4

ISSO-Information System Security Officer CIO2 and 4

ISSE-Information System Security Engineer CIO 2 and 4 and NORESO Cyber Team

Operators-Construction and O&M

CPT-Computer Protection Team-Services, CYBERCOM, NSA

Threat-Response Procedures

b. Threat-Response Procedures (Detection, Mitigation, and Recovery).

Detection Procedures (enclosure A) are designed to enable ICS and IT personnel to identify malicious network activity using official notifications or anomalous symptoms (not attributed to hardware or software malfunctions). While the TTP prescribes certain functional areas in terms of ICS or IT, in general each section is designed for execution by the individuals responsible for the operations of the equipment, regardless of formal designations. **Successful Detection of cyber anomalies is best achieved when IT and ICS managers remain in close coordination.** The *Integrity Checks Table* (enclosure A, section A.3, table A.3.1) lists the procedures to use when identifying malicious cyber activity.

ENCLOSURE A: DETECTION PROCEDURES

AQ1177

ENCLOSURE A: DETECTION PROCEDURES

A.1. Event Diagnostics

A.1.1 Event Diagnostic Table			
Section	Event	Description	Page
A.2.1	Notification	Cyber threat notifications are issued by a variety of entities, including USCYBERCOM, ICS-2014, or the command division.	A-6
Server/Workstation Anomalies			
A.2.2	Log File Check: Unusual Account Usage/Activity	Any log, server or workstation, including SCADA equipment, that shows account use includes: 1. Unusual times user logging in. 2. Rapid logins or continuous logins. 3. User logging into accounts outside of normal working hours. 4. Password failed login attempts. 5. User accounts attempting to execute security privileges.	A-8
A.2.3	Irregular Process Found	On any computer based device, workstation, including SCADA equipment, an irregular process was found.	A-7
A.2.4	Suspicious Software Configurations	Suspicious software and/or configurations were detected on a server or workstation.	A-8
A.2.5	Irregular Audit Log Entry (Or Missing Audit Log)	Applies to any computer based tool, including SCADA equipment, which generates an audit log. Irregular audit log entry may include the following: audit log entries, data or data is not of sequence, data or data is missing from an entry, users that do not log in, security event logs, or log file content.	A-9
A.2.6	Unusual System Behavior	Any tool, including SCADA equipment: 1. Experience reboot or system power change. 2. Unusual low performance or usage of the central processing unit (CPU). 3. CPU cycle up or cycle down for no apparent reason. 4. Inconsistent use of mouse or keyboard. 5. Unusual power fluctuations with the power system. 6. Configuration changes to software made without user or system administrator. 7. System anomalies.	A-10
A.2.7	Asset Is Scanning Other Network Assets	Networks (HMI, PLC, OPC, object linking and embedding (OLE) for distributed control (OLC) or personal devices) have been used or misused as listed below in the ITC data flow baseline. When an asset is communicating outside the bounds of the data flow baseline.	A-12

Enclosure A: Detection Procedures A-1

Notification

A.2.1 Notifications

Server/Workstation Anomalies

A.2. Event Diagnostic Procedures

A.2.2 Server/Workstation: Log File Check: Unusual Account Usage/Activity

A.2.3 Server/Workstation: Irregular Process Found

A.2.4 Server/Workstation: Suspicious Software/Configurations

A.2.5 Server/Workstation: Irregular Audit Log Entry (Or Missing Audit Log)

A.2.6 Server/Workstation: Unusual System Behavior

A.2.7 Server/Workstation: Asset Is Scanning Other Network Assets

A.2.8 Server/Workstation: Unexpected Behavior: HMI, OPC, and Control Server

DETECTION PROCEDURES SERVER EXAMPLE 1

A.1.1 Event Diagnostics Table			
Section	Event	Description	Page
Notification			
A.2.1	Notifications	Cyber event notifications are issued by a variety of entities, including USCYBERCOM, ICS-CERT, or the command directives.	A-5
Server/Workstation Anomalies			
A.2.2	Log File Check: Unusual Account Usage/Activity	Any host server or workstation, including SCADA equipment. Anomalous entries can include: <ol style="list-style-type: none"> 1. Unauthorized user logging in. 2. Rapid and/or continuous log-ins/log-outs. 3. Users logging into accounts outside of normal working hours. 4. Numerous failed log-in attempts. 5. User accounts attempting to escalate account privileges. 	A-6
A.2.3	Irregular Process Found	On any computer-based server, workstation(s), including SCADA equipment, an irregular process was found.	A-7
A.2.4	Suspicious Software/Configurations	Suspicious software and/or configurations were Detected on a server or workstation.	A-8
A.2.5	Irregular Audit Log Entry (or Missing Audit Log)	Applies to any computer-based host, including SCADA equipment, which generates an audit log. Irregular audit log entry may involve the following entries: log is empty, date or time is out of sequence, date or time is missing from an entry, unusual access logged, security event logged, or log file deleted.	A-9
A.2.6	Unusual System Behavior	Any host, including SCADA equipment. <ol style="list-style-type: none"> 1. Spontaneous reboots or screen saver change. 2. Unusually slow performance or usually active central processing unit (CPU). 3. CPU cycles up and cycles down for no apparent reason. 4. Intermittent loss of mouse or keyboard. 5. Configuration files changed without user or system administrator action in operating system. 6. Configuration changes to software made without user or system administrator action. 7. System unresponsive. 	A-10
A.2.7	Asset is Scanning Other Network Assets	Human-machine interfaces (HMI), object linking and embedding (OLE) for process control (OPC), or peripheral devices have known communication paths identified in the FMC data flow baseline. When an asset is communicating outside the bounds of the data flow baseline.	A-12

DETECTION PROCEDURES SERVER EXAMPLE 1

A.2.3 Server/Workstation: Irregular Process Found	
<ul style="list-style-type: none">• Functional Area: IT or ICS• Description: On any computer-based server, workstation, including SCADA equipment, an irregular process was found	
Step	Procedures
Investigation	<ol style="list-style-type: none">1. DETERMINE if the new process belongs to an authorized installation:<ol style="list-style-type: none">a. New software was installed on to the system?b. Was maintenance performed on the system, and if the new process was installed during that maintenance?c. Is the new process a result of a patch update?
No Action Required	<ol style="list-style-type: none">2. If the new process belongs to an authorized installation:<ol style="list-style-type: none">a. DOCUMENT the Severity Level as None (0) in the Security Log.b. CONTINUE with the next diagnostic procedure. If all applicable procedures have been completed, RETURN to <i>Routine Monitoring</i>.
If Action Required	<ol style="list-style-type: none">3. If the new process does not belong to an authorized installation:<ol style="list-style-type: none">a. DOCUMENT in Security Log.b. GO TO Section A.3, A.3.1 <i>Integrity Checks Table</i>. (See recommended checks below.) LOCATE the integrity check associated with server or workstation you are investigating and EXECUTE the Integrity checks. Recommended Checks:<ul style="list-style-type: none">A.3.2.1 Server/Workstation Process CheckA.3.2.2 Server/Workstation Log ReviewA.3.2.4 Server/Workstation Communications CheckA.3.2.16 Peripherals Integrity CheckA.3.2.9 Controller Integrity CheckA.3.2.13 Server/Workstation Rootkit Check4. Once you have completed all appropriate Integrity Checks, GO TO section A.2.29 Action Step.

DETECTION PROCEDURES SERVER EXAMPLE 1

The screenshot displays the GlassWire Alerts window. The interface includes a top navigation bar with tabs for Graph, Firewall, Usage, Network, and Alerts. Below this is a header with columns for Date, Apps, and Type, and a 'Mark all as read' button. The main area shows a list of alerts for August 29th, with a red oval highlighting the application details on the right side.

Date	Apps	Type
Aug 29		
1:29 pm		Application info changed The application executable changed.
1:29 pm		First network activity First network connection initiated.
10:14 am		First network activity First network connection initiated.
10:11 am		Application info changed The application version changed from "1.2.71" to "1.2.73".
9:55 am		Application info changed The application version changed from "16.0.7070.2030" to "16.0.7167.2040".
8:36 am		Application info changed The application version changed from "16.0.7070.2030" to "16.0.7167.2040".
8:34 am		Application info changed The application version changed from "16.0.7070.1323" to "16.0.7167.1332".
8:34 am		Application info changed

The application details highlighted in the red oval include:

- Cisco WebEx Service
- global-network.webex.com
- Cisco WebEx Meeting Download
- 52.36.248.120
- Remote Desktop Connection
- GlassWire Control Service
- Microsoft Word
- Office Subscription Licensing Heartbeat
- Microsoft Office Click-to-Run Integrator

The Windows taskbar at the bottom shows the system tray with the time 2:13 PM and date 8/29/2016.

DETECTION PROCEDURES SERVER EXAMPLE 1

A.3.2.1 Server/Workstation Process Check	
<ul style="list-style-type: none"> • Who should do this check: The organization or individual responsible for the server or workstation • What is needed for this check: <ol style="list-style-type: none"> 1. FMC data flow chart 2. FMC baseline topology 3. FMC baseline authorized process and tasks 4. FMC baseline software list 5. FMC baseline system information 	
Step	Procedures
1.	<p>If the machine is responsive, EXECUTE steps a and b below. Once completed, RETURN to this section, and resume with Step 2.</p> <ol style="list-style-type: none"> a. Section: A.3.2.2 Server/Workstation Log Review. b. Section: A.3.2.3 Unauthorized User Account Activity. <p>If the machine is not responsive, GO TO Section A.3.2.5 <i>Server/Workstation Unresponsive Check</i>.</p>
2.	<p>If Procedures A.3.2.2 or A.3.2.3 do not result in a Severity Level of High (3), CONTINUE to step 3.</p>
3.	<p>Process Check: LAUNCH SysInternals: CHECK for processes that do not appear legitimate. This can include (but is not limited to) processes that:</p> <ol style="list-style-type: none"> a. Have no icon or name. b. Have no descriptive or company name. c. Are unsigned Microsoft images. d. Reside in the Windows directory. e. Include strange uniform resource locators (URLs) in their strings. f. Communicating with unknown IP address (use FMC data flow diagram to compare). g. Host suspicious dynamic link library (DLL) or services (hiding as a DLL instead of a process). h. LOOK for "packed" processes which are highlighted in purple.
4.	<p>If an anomalous process was found:</p> <ol style="list-style-type: none"> a. DOCUMENT details of the event in Security Log. b. CONTACT system administrator responsible for the machine or the command ISSM. <ol style="list-style-type: none"> (1) REPORT suspicious process. (2) REQUEST assistance in determining if the process is malicious (process may be undocumented but normal). (3) If the process is not malicious, DOCUMENT in Security Log, and EXECUTE A.3.2.4 Server/Workstation Communications Check. (4) If the process is malicious, DOCUMENT the Severity Level of High (3) in the Security log. c. GO TO section A.2.29 Action Step.
5.	<p>If an anomalous process was not found:</p> <ol style="list-style-type: none"> a. DOCUMENT the Severity Level as None (0). b. RETURN to the previous diagnostic procedure and continue with <i>Recommended Checks</i>.

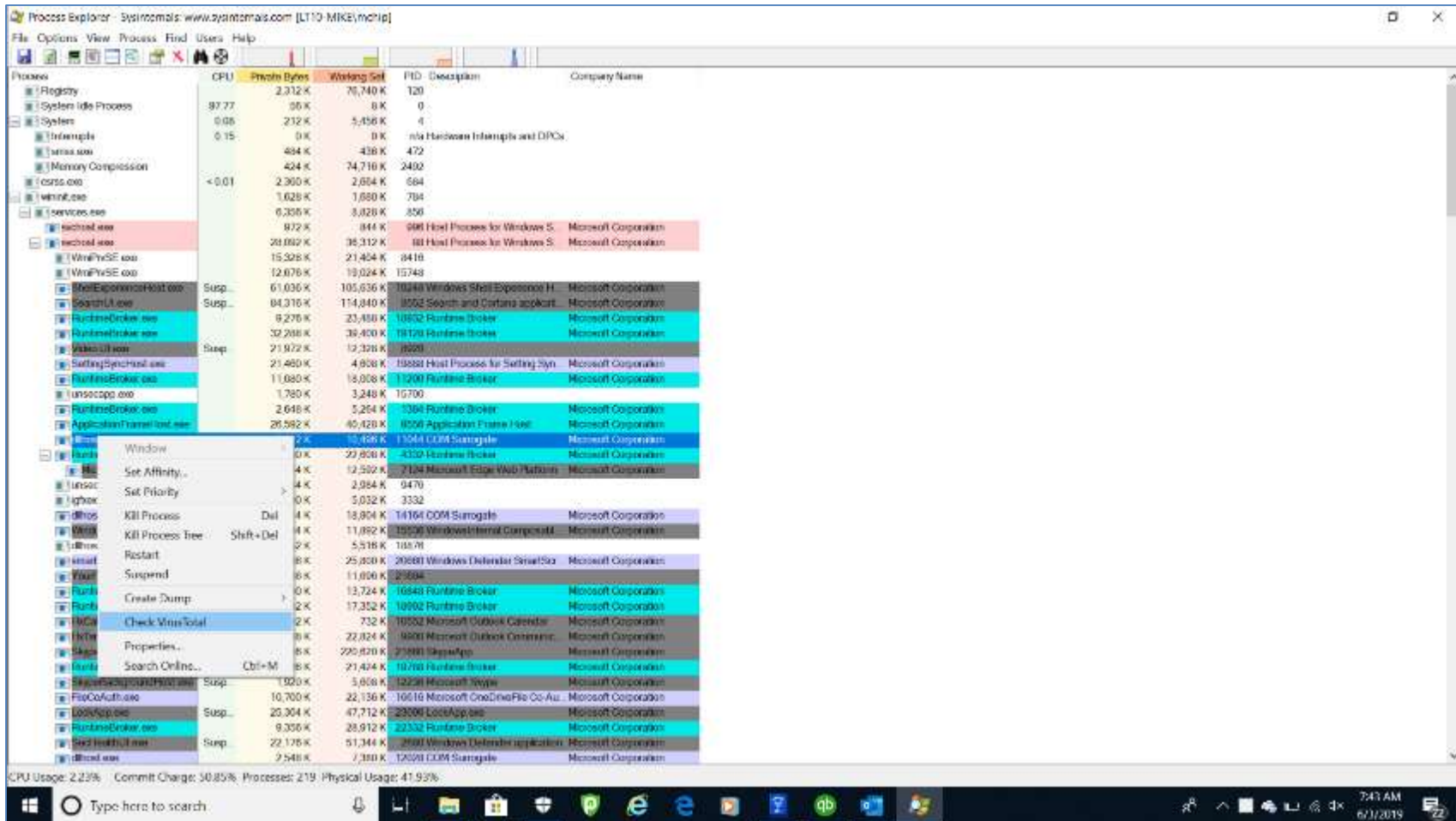
DETECTION PROCEDURES SERVER EXAMPLE 1

The screenshot displays the MS Process Explorer interface. The main window shows a list of processes with columns for CPU usage, Private Bytes, Working Set, PID, and Description. A 'System Information' dialog box is open, showing system metrics such as System Commit (4.9 GB), Physical Memory (4.4 GB), and Commit Charge (35.97%). Two blue circles highlight specific processes in the list: 'OASFramework45.exe' and 'OPCSysData.exe' in the upper circle, and 'OPCSysDatabase.exe' in the lower circle. The taskbar at the bottom shows the system tray with the time 2:01 PM on 8/29/2016.

Process	CPU	Private Bytes	Working Set	PID	Description
svchost.exe	< 0.01	2,584 K	8,832 K	1088	Host Pr...
svchost.exe	1.51	21,448 K	21,448 K	3932	
svchost.exe		4,188 K	13,284 K	1778	Host Pr...
svchost.exe		5,124 K	15,388 K	1904	Host Pr...
wlanacd.exe		4,832 K	16,060 K	3544	
lcomhost.exe		1,120 K	4,804 K	3652	
spoolsv.exe	< 0.01	15,168 K	28,192 K	1956	Spooler
QBDFMonitorService.exe		10,616 K	15,872 K	2156	QuickB...
EvtEng.exe	< 0.01	4,436 K	13,204 K	2208	Inte(R)...
OASFramework45.exe	0.24	15,180 K	20,500 K	2218	OAS Fr...
lsisrv.exe		358 K	4,018 K	2240	Inte(R)...
OPCSysData.exe	0.07	29,132 K	24,536 K	2284	OPCSy...
mbamservice.exe	0.02	24,172 K	225,048 K	2292	Malwar...
mbam.exe	0.15	34,568 K	59,540 K	6280	
mbamscheduler.exe		5,064 K	12,184 K	2300	Malwar...
ZenOSOnlineService.exe		4,644 K	16,876 K	2312	Inte(R)...
vmtoolsd.exe	< 0.01	1,712 K	6,514 K	2324	VMware
vmtoolsdproc.exe		7,344 K	4,528 K	2332	VMware
svchost.exe		7,084 K	19,800 K	2340	Host Pr...
vmware-authd.exe		4,724 K	11,432 K	2408	VMware
vmtoolsd.exe	< 0.01	2,312 K	9,596 K	2418	VMware
sqlwriter.exe		1,912 K	7,336 K	2432	SQL Se...
svchost.exe		2,912 K	8,000 K	2460	Host Pr...
QBIDPService.exe		8,812 K	14,364 K	2492	QBIDP...
MsMpEng.exe	0.07	163,076 K	123,112 K	2504	Antimal...
OPCSysDatabase.exe	0.49	28,140 K	25,840 K	2580	OPCSy...
RegSvc.exe		1,738 K	8,648 K	2598	Inte(R)...
svchost.exe		10,884 K	29,260 K	2620	Host Pr...
HMP_NSWSV.exe	< 0.02	1,484 K	19,700 K	2780	F-ayMI...
svchost.exe		5,296 K	14,004 K	4268	Host Pr...
NisSrv.exe		11,782 K	8,880 K	5082	Microso...
svchost.exe		6,892 K	25,852 K	5758	Host Process for Windows S...
PresentationFontCache.exe		28,112 K	18,372 K	5948	PresentationFontCache.exe
ePowerSvc.exe		2,288 K	9,438 K	2588	ePowerSvc
ePowerTray.exe	0.08	3,012 K	12,880 K	5324	ePowerTray
ePowerFront.exe	0.08	16,588 K	23,848 K	1192	

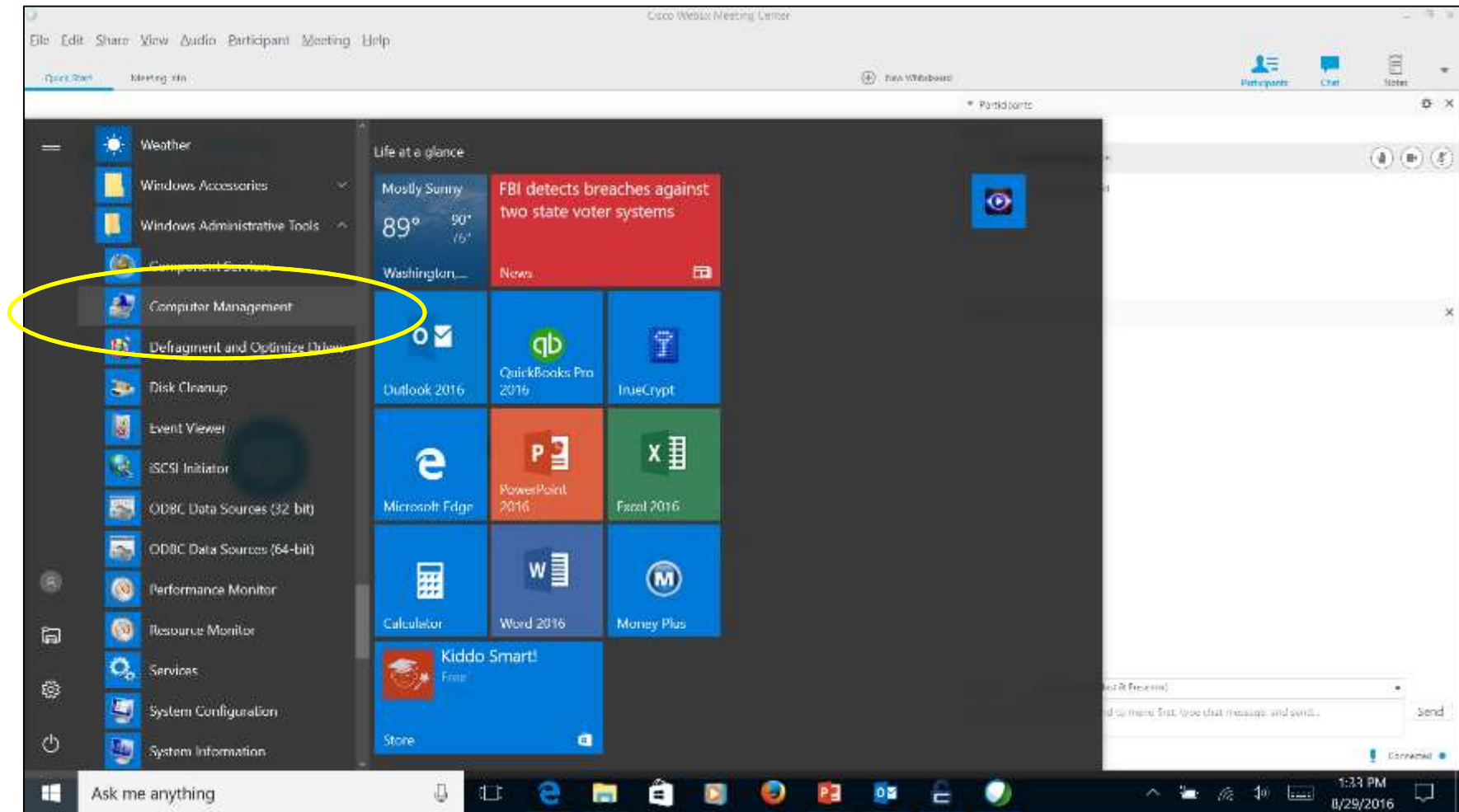
MS Process Explorer

Virus Total – Use with Extreme Caution



DO NOT submit a file to Virus Total unless you want it to be seen by the world forever
But we will use it to check suspicious files.....

DETECTION PROCEDURES SERVER EXAMPLE 1



Windows Administrative Tools Computer Management

DETECTION PROCEDURES SERVER EXAMPLE 1

The screenshot displays the Windows Administrative Tools Computer Management console. The left-hand navigation pane shows the tree structure under 'Event Viewer', with 'Security' highlighted and circled in blue. The main pane shows a list of events with the following columns: Keywords, Date and Time, Source, Event ID, and Task Category. The 'Security' log is selected, and event 4672 is highlighted. A detailed view of event 4672 is shown below the list, including the event description, subject, and metadata.

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	8/29/2016 1:29:14 PM	Microsoft Windows ...	4672	Special Logon
Audit Success	8/29/2016 1:29:14 PM	Microsoft Windows ...	4624	Logon
Audit Success	8/29/2016 1:07:39 PM	Microsoft Windows ...	4634	Logoff
Audit Success	8/29/2016 1:07:29 PM	Microsoft Windows ...	4624	Logon
Audit Success	8/29/2016 12:55:39 PM	Microsoft Windows ...	4634	Logoff
Audit Success	8/29/2016 12:55:28 PM	Microsoft Windows ...	4624	Logon
Audit Success	8/29/2016 12:51:01 PM	Microsoft Windows ...	4672	Special Logon
Audit Success	8/29/2016 12:51:01 PM	Microsoft Windows ...	4624	Logon
Audit Success	8/29/2016 12:46:36 PM	Microsoft Windows ...	4634	Logoff
Audit Success	8/29/2016 12:46:26 PM	Microsoft Windows ...	4624	Logon
Audit Success	8/29/2016 12:43:38 PM	Microsoft Windows ...	4634	Logoff
Audit Success	8/29/2016 12:43:28 PM	Microsoft Windows ...	4624	Logon
Audit Success	8/29/2016 12:34:06 PM	Microsoft Windows ...	4634	Logoff
Audit Success	8/29/2016 12:33:56 PM	Microsoft Windows ...	4624	Logon
Audit Success	8/29/2016 12:33:20 PM	Microsoft Windows ...	4634	Logoff
Audit Success	8/29/2016 12:33:06 PM	Microsoft Windows ...	4624	Logon

Event 4672, Microsoft Windows security auditing.

General Details

Special privileges assigned to new logon.

Subject:

Log Name: Security
Source: Microsoft Windows security Logged: 8/29/2016 1:29:14 PM
Event ID: 4672 Task Category: Special Logon
Level: Information Keywords: Audit Success

Windows Administrative Tools Computer Management Windows Logs

Detect Privilege Escalation

EE.16 Detect Privilege escalation

Malware may attempt to gain privileges on an OS (i.e. from a standard user to administrator) in order to execute tasks that require administrative privileges.

A. Detect Windows Scheduler based or similar attacks (on AT, WinAT), as well as attacks on permissions:

Review Windows Event Log for the following eventIDs and determine if the event(s) were authorized.

- 4648 (security) A logon was attempted using explicit credentials (often used in scripts, scheduled tasks, or with RUNAS command, or to authenticate to a remote host as a different user)
- 4697 (security) A service was installed on the system
- 4698 (security) A scheduled task was created
- 4720 (security) A user account was created
- 4724 (security) An attempt was made to reset an accounts password
- 4728 (security) A member was added to a security-enabled global group
- 4732 (security) A member was added to a security-enabled local group
- 4735 (security) A security-enabled local group was changed

DETECTION PROCEDURES SERVER EXAMPLE 1

The screenshot shows the Windows Computer Management console. The left-hand navigation pane is expanded to 'Storage', where 'Disk Management' is highlighted and circled in blue. The main area displays a table of volumes and a disk layout for Disk 0.

Volume	Layout	Type	File System	Status	Capacity	Free Space	% Free	Actions
	Simple	Basic		Healthy (EFI System Partition)	100 MB	100 MB	100 %	
	Simple	Basic		Healthy (Recovery Partition)	500 MB	500 MB	100 %	
Acer (C:)	Simple	Basic	NTFS	Healthy (Boot, Page File, Crash Dump, Primary Partition)	481.69 GB	419.60 GB	87 %	
Data (E:)	Simple	Basic	NTFS	Healthy (Primary Partition)	390.62 GB	93.33 GB	24 %	
Front Office (F:)	Simple	Basic	NTFS	Healthy (Primary Partition)	58.59 GB	25.23 GB	43 %	

Disk	Layout	Type	File System	Status	Capacity	Free Space	% Free	Actions
Disk 0	Basic	931.50 GB	Online					
	100 MB	Acer (C:)	481.69 GB NTFS	Healthy (Boot, Page File, Crash	58.59 GB NTFS	390.62 GB NTFS	500 MB	Healthy (Recc
		Healthy (Primary Partition)	Healthy (Primary Partition)					

Legend: ■ Unallocated ■ Primary partition

Windows Administrative Tools Computer Management Data Management

Protecting FRCS

- Turn on BitLocker (Full Disk Encryption Data at Rest)
- Ensure Internet Options Transport Layer Security 1.2 and/or 1.3 on (Data encrypted in Transit)
- Update Operating System and Applications (patching)
- Applying the Security Technical Implementation Guides with the SCAP Tool (Hardening)
- Daily Anti-Virus Malware Scan (Windows Security or HBSS/ACAS/ESS)
- Regular Vulnerability Scans (HBSS/ACAS/ESS)
- Regular Password Changes (enforced by the STIGS)
- Regular System Checks by Operators (Computer Management, Disk Health, Event Logs)
- Maintain the Configuration Baseline Audit Reports (Quarterly per contract)
- Practice using the DoD Advanced Industrial Control Systems Tactics, Techniques and Procedures (Hunt and Defend 101)

Protecting FRCS Resources

CompTIA Security +

Cisco CNNA

DHS CISA

DoD ESTCP Cybersecuring FRCS Website

SANS

GIAC GICSP

Whole Building Design Guide Cybersecurity Website

DOE Energy Exchange Conference Cyber Tracks

SAME Cyber Resilience IGE

SAME JETC Conference

Vendor Newsletters

The need for Cyber Warriors in the OT/FRCS space will continue to increase; understanding what the Components and Devices are, how they function, how they are connected, how to harden them, how to establish the Configuration Baseline and Normal Behavior and then Identify and Mitigate Abnormal Behavior are challenging.

Next Phase Coming – Quantum Computing and AI – SkyNet is not far away....

QUESTIONS



Michael Chipley
President, The PMC Group LLC
Cell: 571-232-3890
E-mail: mchipley@pmcgroup.biz