AABC Commissioning Group

AIA Provider Number 50111116

Your Control Systems Have Been Hacked, Now What?

Course Number: CXENERGY1717

Michael Chipley, Ph.D., GICSP, PMP, LEED AP
The PMC Group LLC
Eric Nickel, GICSP, RCDD, CEP, CEH
Chinook Systems

April 26, 2017

Credit(s) earned on completion of this course will be reported to AIA CES for AIA members. Certificates of Completion for both AIA members and non-AIA members are available upon request.

This course is registered with AIA CES for continuing professional education. As such, it does not include content that may be deemed or construed to be an approval or endorsement by the AIA of any material of construction or any method or manner of handling, using, distributing, or dealing in any material or product.

Questions related to specific materials, methods, and services will be addressed at the conclusion of this presentation.

Copyright Materials

The PMC Group LLC

Engineering a better tomorrow today

Course Description

This presentation is an overview of the Advanced Control System Tactics, Techniques and Procedures (TTPs) developed by the U.S. Cyber Command. Control System owners, facility managers, engineering, physical security, information assurance and other professionals involved with the design, deployment and operation of Control Systems need to learn how to detect, contain, eradicate and recover from a cyber-attack specifically targeting Control Systems.

Learning Objectives

At the end of the this course, participants will be able to:

1. Learn how to find Control Systems exposed on the internet using Google Hacking, Shodan, and WhiteScope discovery tools.

2. Learn how to detect, contain, eradicate and recover from a cyber-attack specifically targeting Control Systems.

3. Learn how to build a Recovery Jump-Kit, use it to find and eradicate malware using tools such as MalwareBytes and the Microsoft Internals suite, and perform Control Systems forensics data collection.

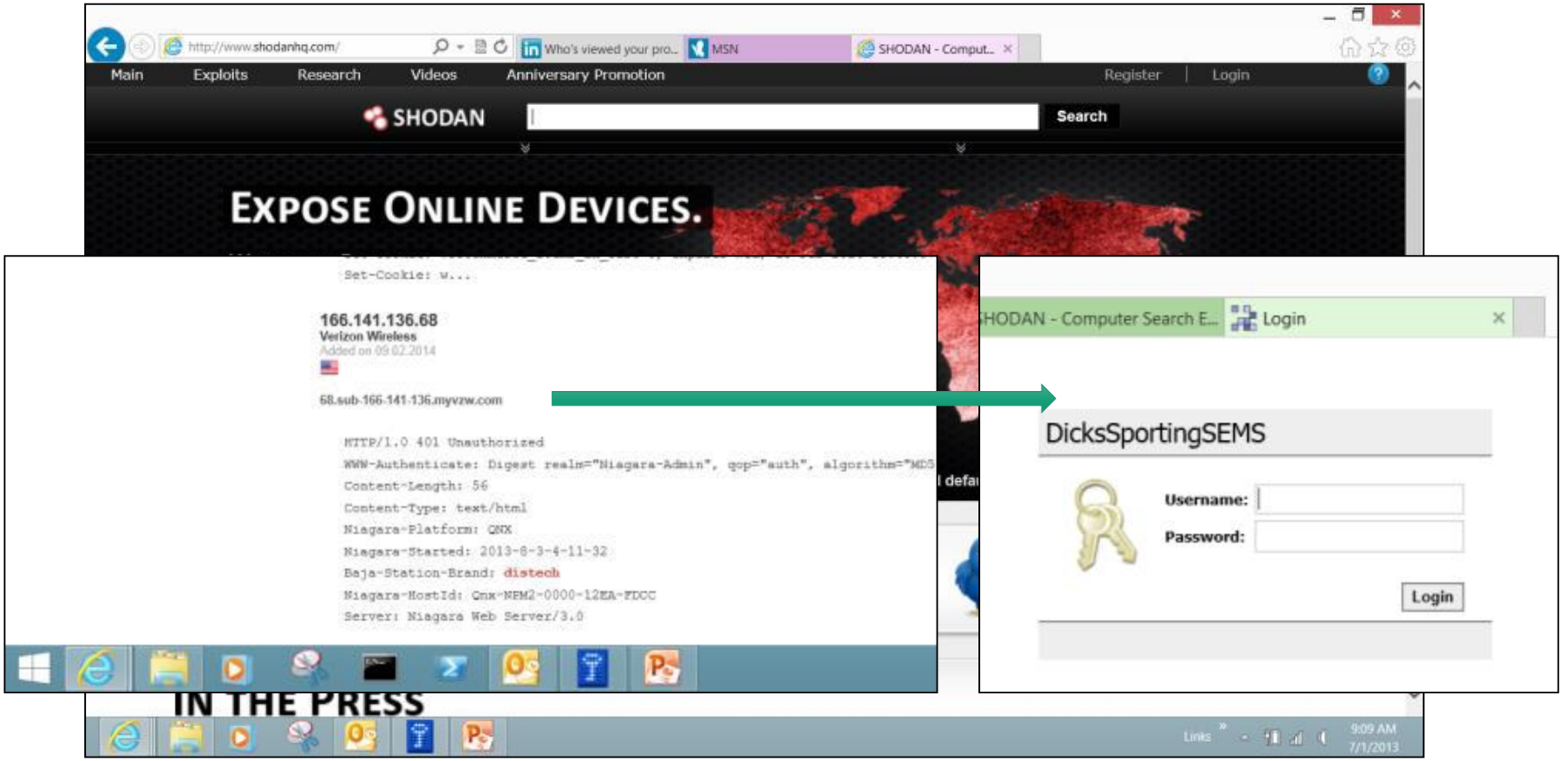
4. Learn how to evaluate the cyber severity of the event/incident and prepare an incident report.

Overview

- DoD CIO C&A Transformation
- NIST SP 800-53 and SP 800-82, CNSSI 1253
- DHS Cybersecurity Evaluation Tool (CSET)
- DoD RMF KS CS PIT website
- eMASS with CS PIT Step-By Step Manual Method
- DHS Interagency Security Committee Converged Systems
- Acquisition/Procurement
- Cyber Workforce Skills and Credentials, Ranges
- Continuous Monitoring, Alerts and Advisories
- Cybersecuring DoD CS Workshop

OT IP Controllers are in Everything

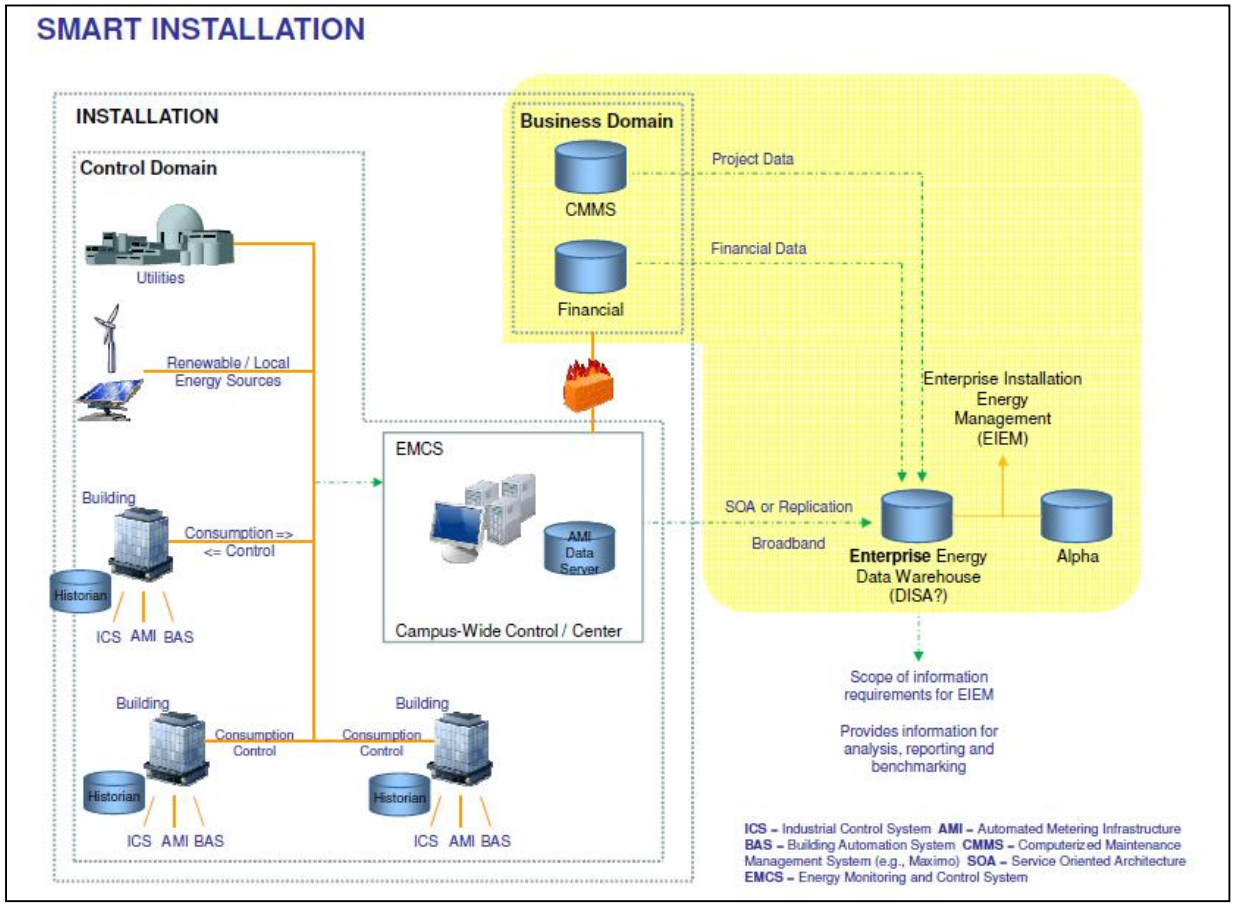
Shodan Site = Locates CS



Many CS systems directly connected to internet with no protection, Only http

In the Beginning….2010

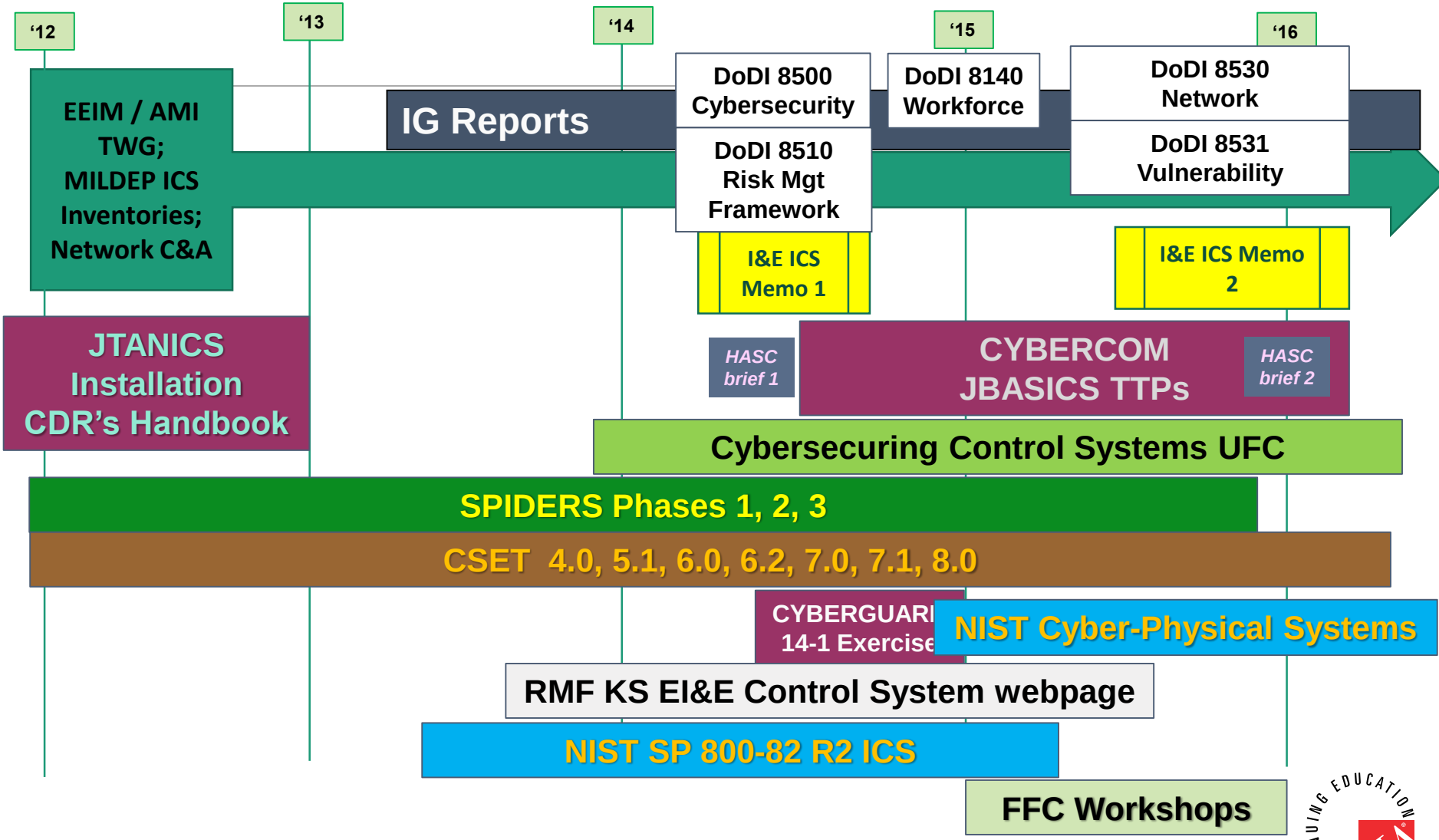
A great idea rudely interrupted by reality…CIO AMI ATO denial and Stuxnet



OSD Energy, Installations and Environment

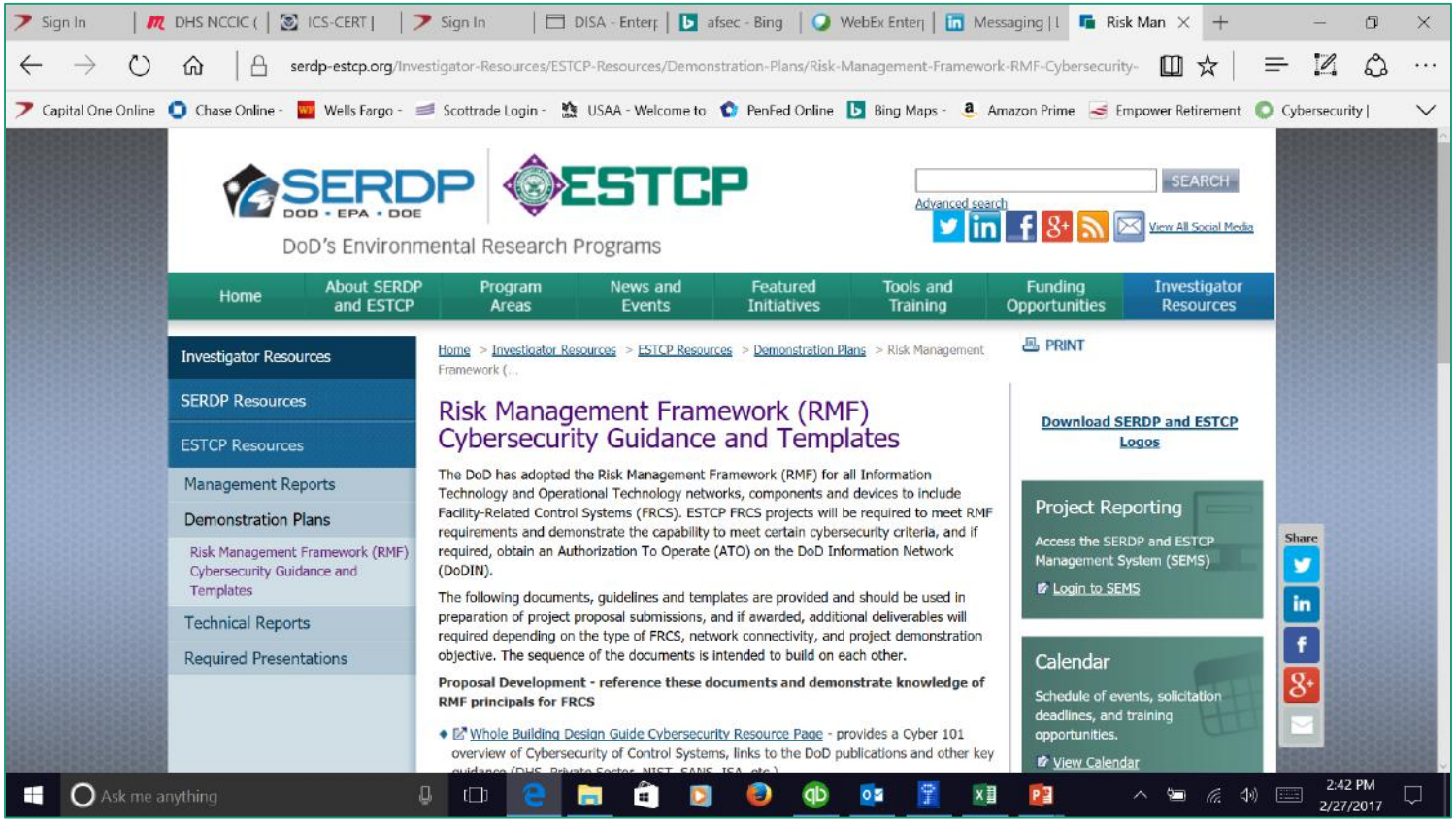
OSD role is to provide clear policy and guidance…

EI&E Cybersecurity Efforts



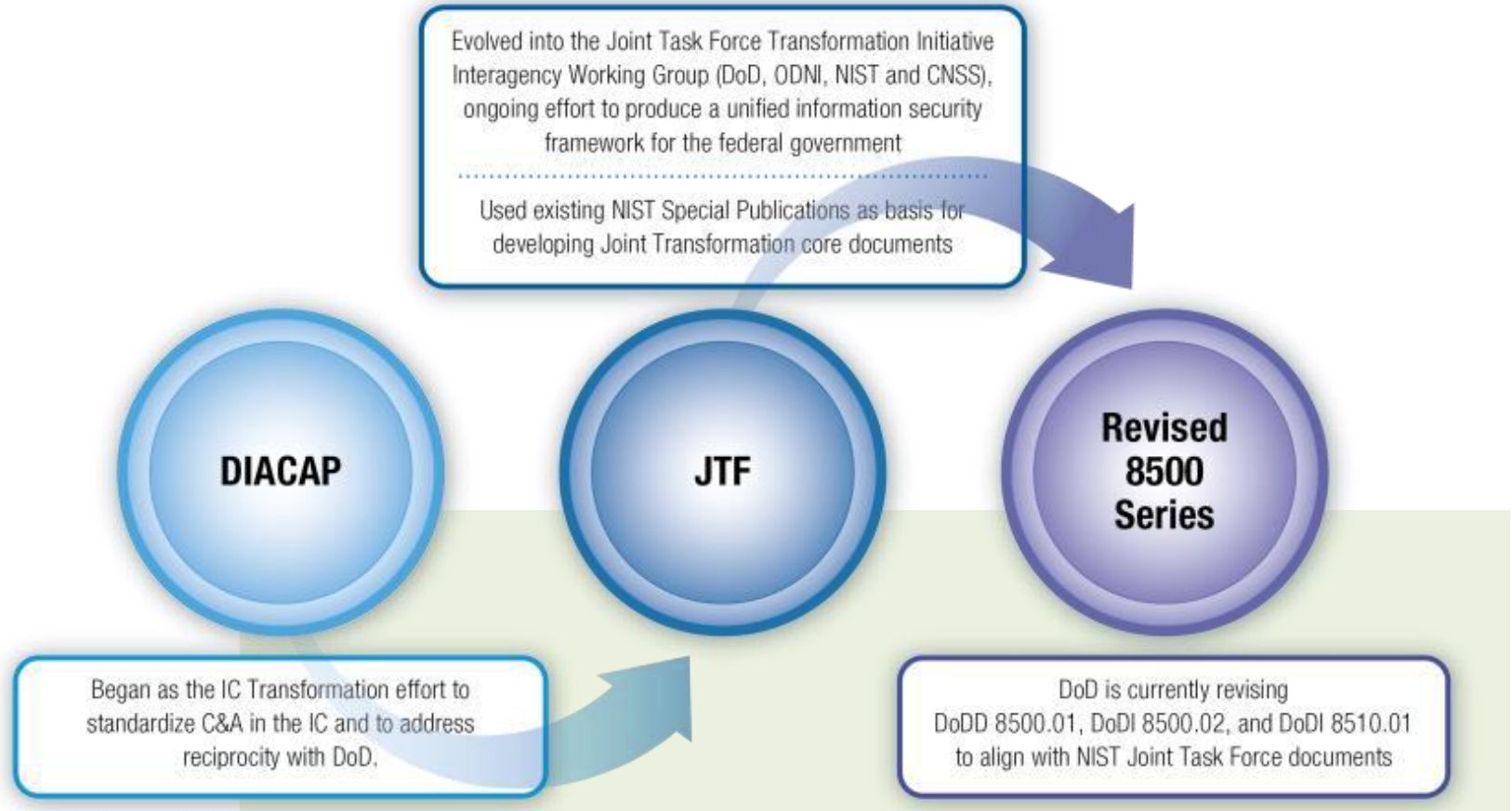
Many Stakeholders; DoD Policy, Experiment, Exercise Roles

RMF Facilities-Related Cybersecurity Guidance and Templates



https://www.serdp-estcp.org/Investigator-Resources/ESTCP-Resources/Demonstration-Plans/Risk-Management-Framework-RMF-Cybersecurity-Guidance-and-Templates

DoDI 8500.01 and 8510.01 Update

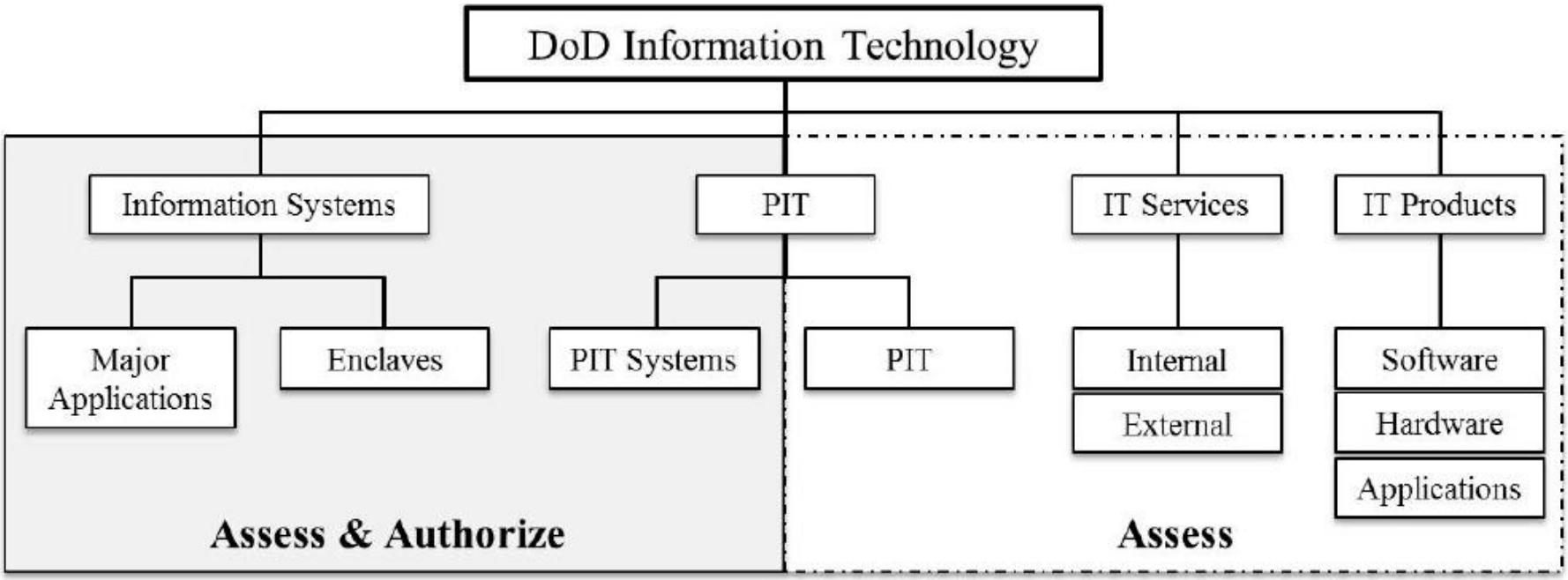


Transition Bottom Line – DoD will continue to follow the DoD 8500 series documentation for information assurance and risk management processes, procedures, and guidance

PIT, PIT Systems, PIT Stand-Alone

DoDI 8510.01 “Risk Management Framework for DoD IT”
- Provides clarity regarding what IT should undergo the RMF process and how

Figure 1. DoD IT



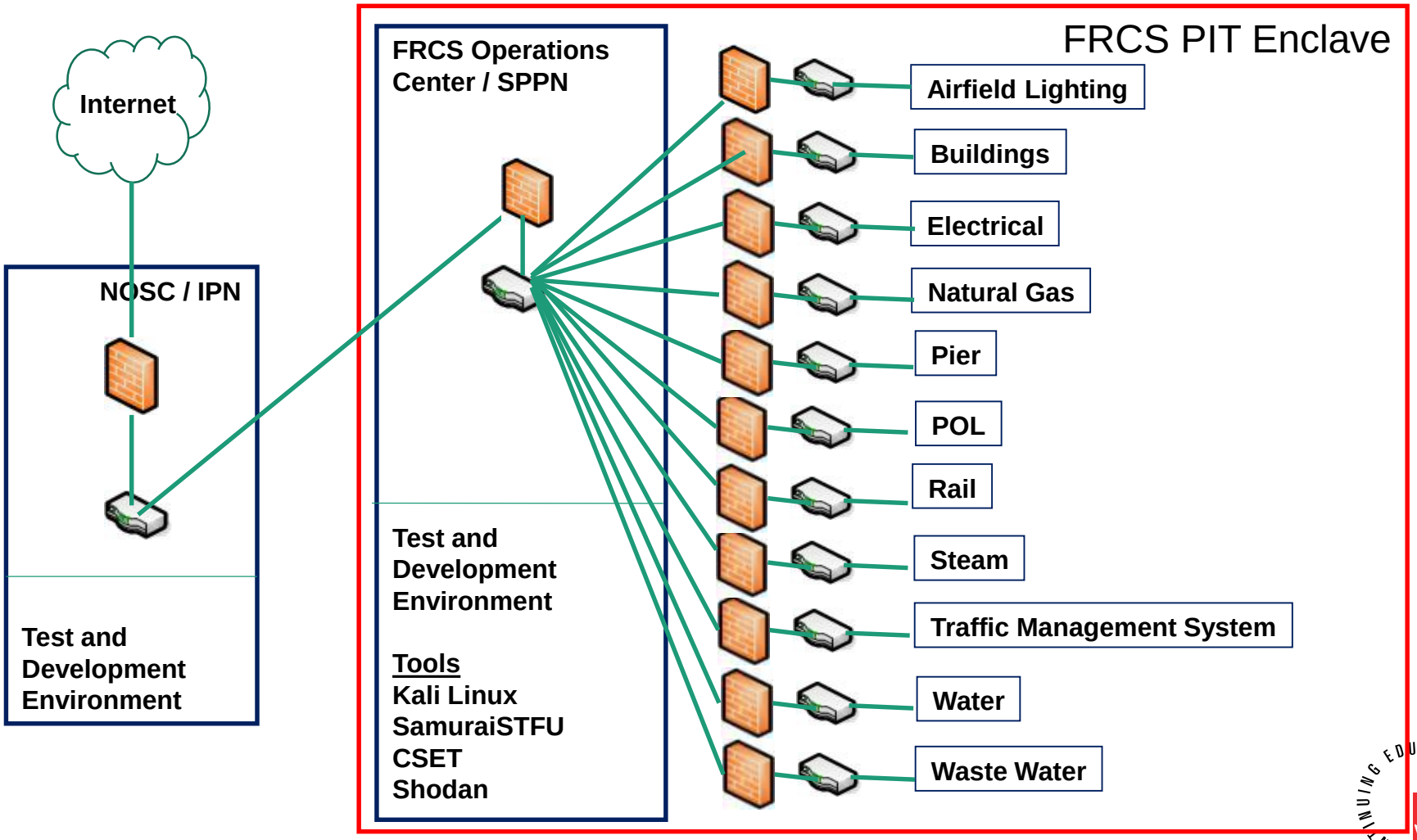
AA = Full 6 steps of RMF, A = 4 steps of RMF

DoDI 8500.01 PIT Examples

(b) Examples of platforms that may include PIT are: weapons systems, training simulators, diagnostic test and maintenance equipment, calibration equipment, equipment used in the research and development of weapons systems, medical devices and health information 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 including 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).

Installations and Environment worked with CIO to expand definition of PIT systems, then added to NIST SP 800-82R2 – 3 years in the making

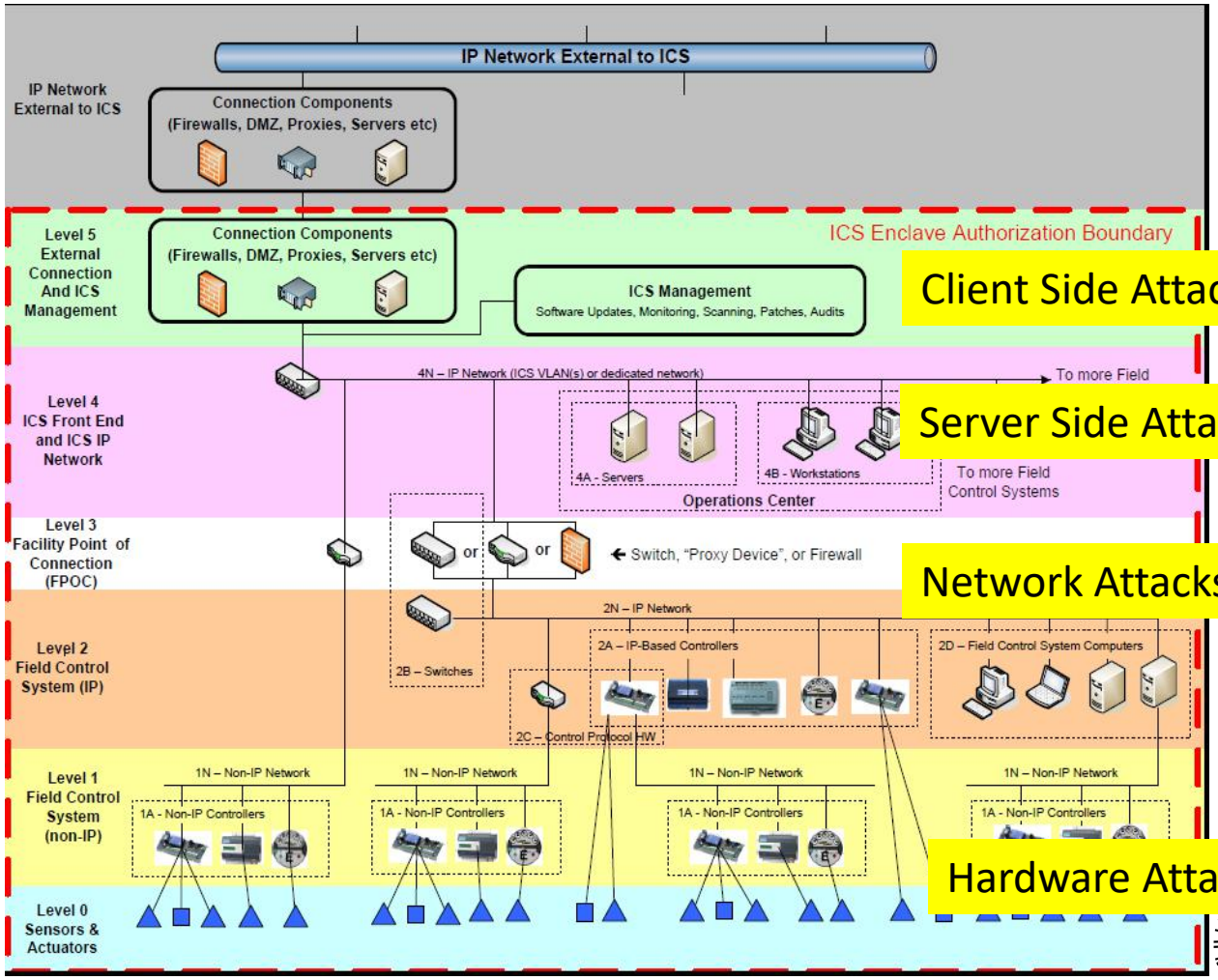
DoD FRCS Systems and the Joint Information Environment (JIE)



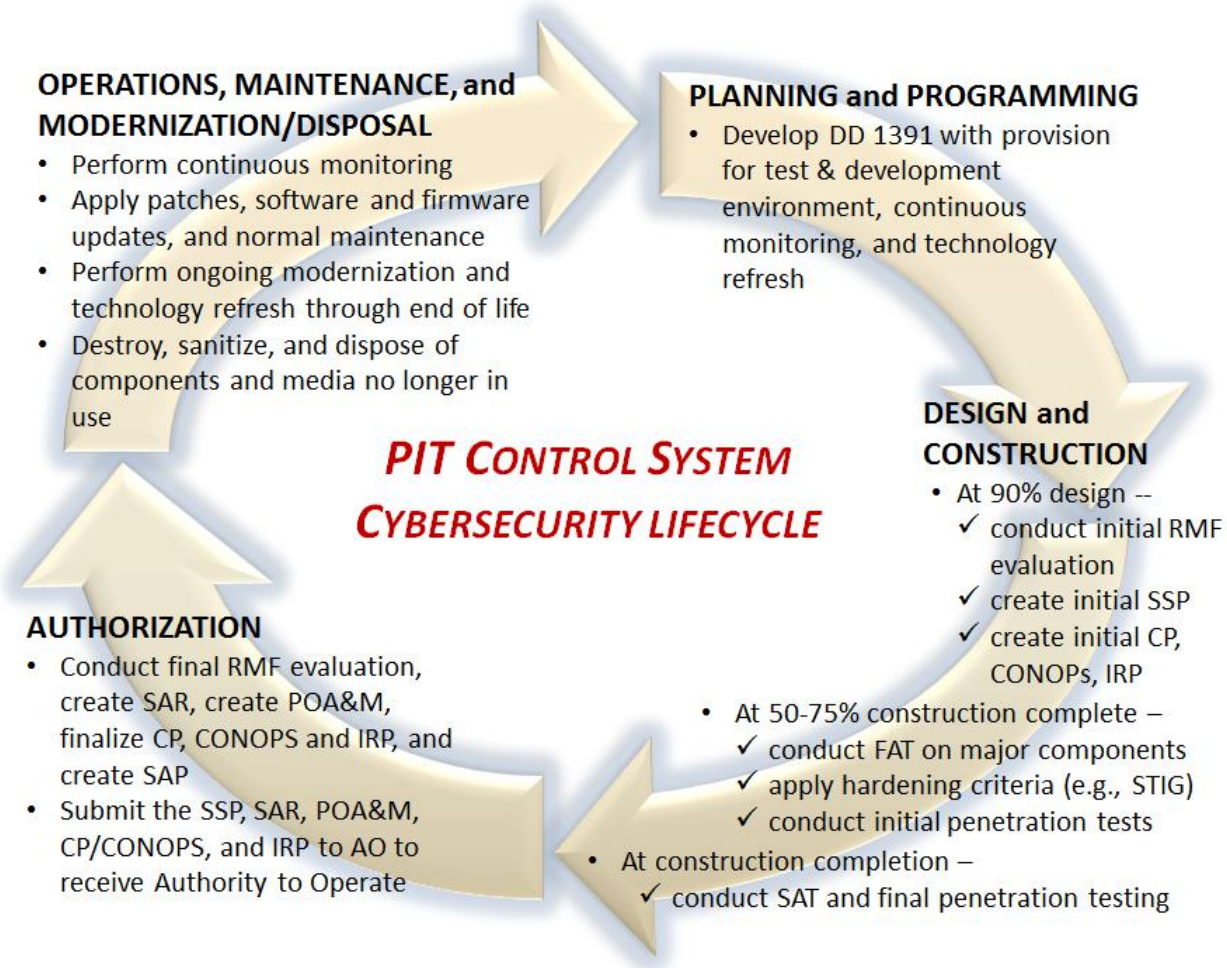
CS Monitoring and Network Attack Points

Host Based Security Systems Scanning (Active)
Windows, Linux
HTTP, TCP, UDP

Intrusion Detection Systems (Passive)
PLC, RTU, Sensor
Modbus, LonTalk, BACNet, DNP 3



PIT Control System Cyber Lifecycle



NIST SP 800-82 Rev 2 May 2015

This document provides guidance for establishing secure industrial control systems (ICS). These ICS, which include supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as skid-mounted Programmable Logic Controllers (PLC) are often found in the industrial control sectors.

This document provides an overview of these ICS and typical system topologies, identifies typical threats and vulnerabilities to these systems, and provides recommended security countermeasures to mitigate the associated risks.

800-82 Rev 2 - **Appendix G ICS Overlay uses the 800-53 security controls and adds Supplemental Guidance:**

"Instead of Screen Lock after 15 minutes of inactivity, use 2 person control"

A special acknowledgement to Lisa Kaiser, Department of Homeland Security, the Department of Homeland Security Industrial Control System Joint Working Group (ICSJWG), and Office of the Deputy Undersecretary of Defense for Installations and Environment, Business Enterprise Integration Directorate staff, **Daryl Haegley and Michael Chipley**, for their exceptional contributions to this publication.

Standards - NIST SP 800-82R2 2015

2.5 Other Types of Control Systems

Although this guide provides guidance for securing ICS, other types of control systems share similar characteristics and many of the recommendations from this guide are applicable and could be used as a reference to protect such systems against cybersecurity threats. For example, although many building, transportation, medical, security and logistics systems use different protocols, ports and services and are configured and operate in different modes than ICS, they share similar characteristics to traditional ICS [18]. Examples of some of these systems and protocols include:

Other Types of Control Systems

- Advanced Metering Infrastructure
- Building Automation System
- Building Management Control System
- CCTV Surveillance System
- CO2 Monitoring
- Digital Signage Systems
- etc

Protocols/Ports and Services

- Modbus: Master/Slave - Port 502
- BACnet: Master/Slave - Port 47808
- LonWorks/LonTalk: Peer to Peer - Port 1628/29
- DNP3: Master/Slave - Port 20000
- IEEE 802.x - Peer to Peer
- Zigbee - Peer to Peer
- Bluetooth – Master/Slave

http://csrc.nist.gov/

NIST SP 800-82R2 Key Security Controls

Inventory
- CM-8 Information System Component Inventory
- PM-5 Information System Inventory
- PL-7 Security Concept of Operations
- PL-8 Information Security Architecture
- SC-41 Port and I/O Device Access
- PM-5 Information System Inventory

Central Monitoring
- AU-6 Audit Review, Analysis, and Reporting
- CA -7 Continuous Monitoring
- IR-5 Incident Monitoring
- IR-6 Incident Reporting
- PE-6 Monitoring Physical Access
- PM-14 Testing, Training and Monitoring
- RA-5 Vulnerability Scanning
- SC-7 Boundary Protection
- SI-4 Information System Monitoring
- SI-5 Security Alerts, Advisories, and Directives

Test and Development Environment
- CA-8 Penetration Testing
- CM-4 Security Impact Analysis
- CP-3 Contingency Training
- CP-4 Contingency Plan Testing and Exercises
- PM-14 Testing, Training and Monitoring

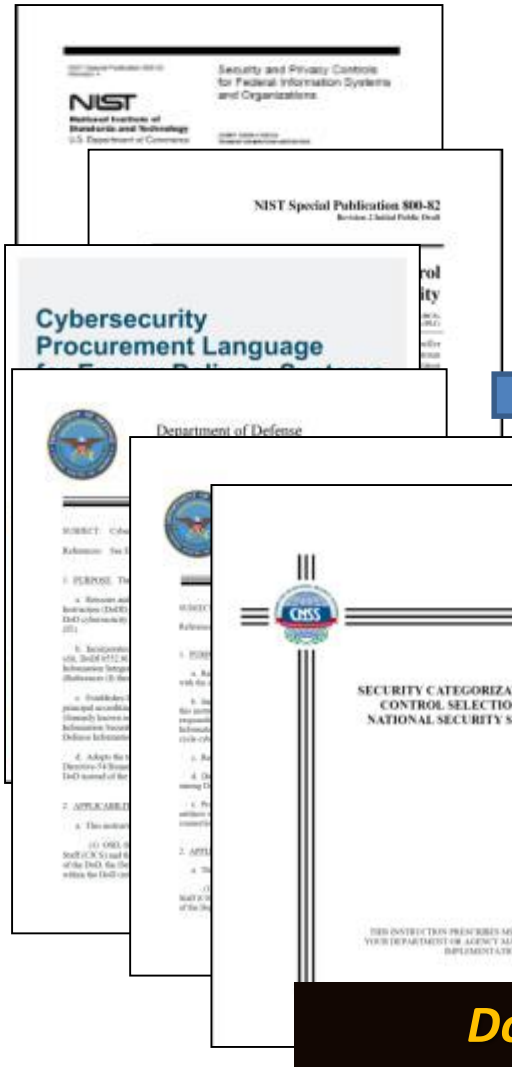
Critical Infrastructure
- CP-2 Contingency Plan
- CP-6 Alternate Storage Site
- CP-7 Alternate Processing Site
- CP-10 Information System Recovery and Reconstitution
- PE-3 Physical Access Control
- PE-10 Emergency Shutoff
- PE-11 Emergency Power
- PE-12 Emergency Lighting
- PE-13 Fire Protection
- PE-14 Temperature and Humidity Controls
- PE-17 Alternate Work Site
- PM-8 Critical Infrastructure Plan

Acquisition and Contracts
- AU-6 Audit Review, Analysis, and Reporting
- CA -7 Continuous Monitoring
- SA-4 Acquisitions
- PM-3 Information System Resources
- PM-14 Testing, Training and Monitoring

Inbound Protection, Outbound Detection

DHS Cyber Security Evaluation Tool (CSET) for CS Self-Assessments

CSET has DoD, CNSS, NIST and DHS documents and processes

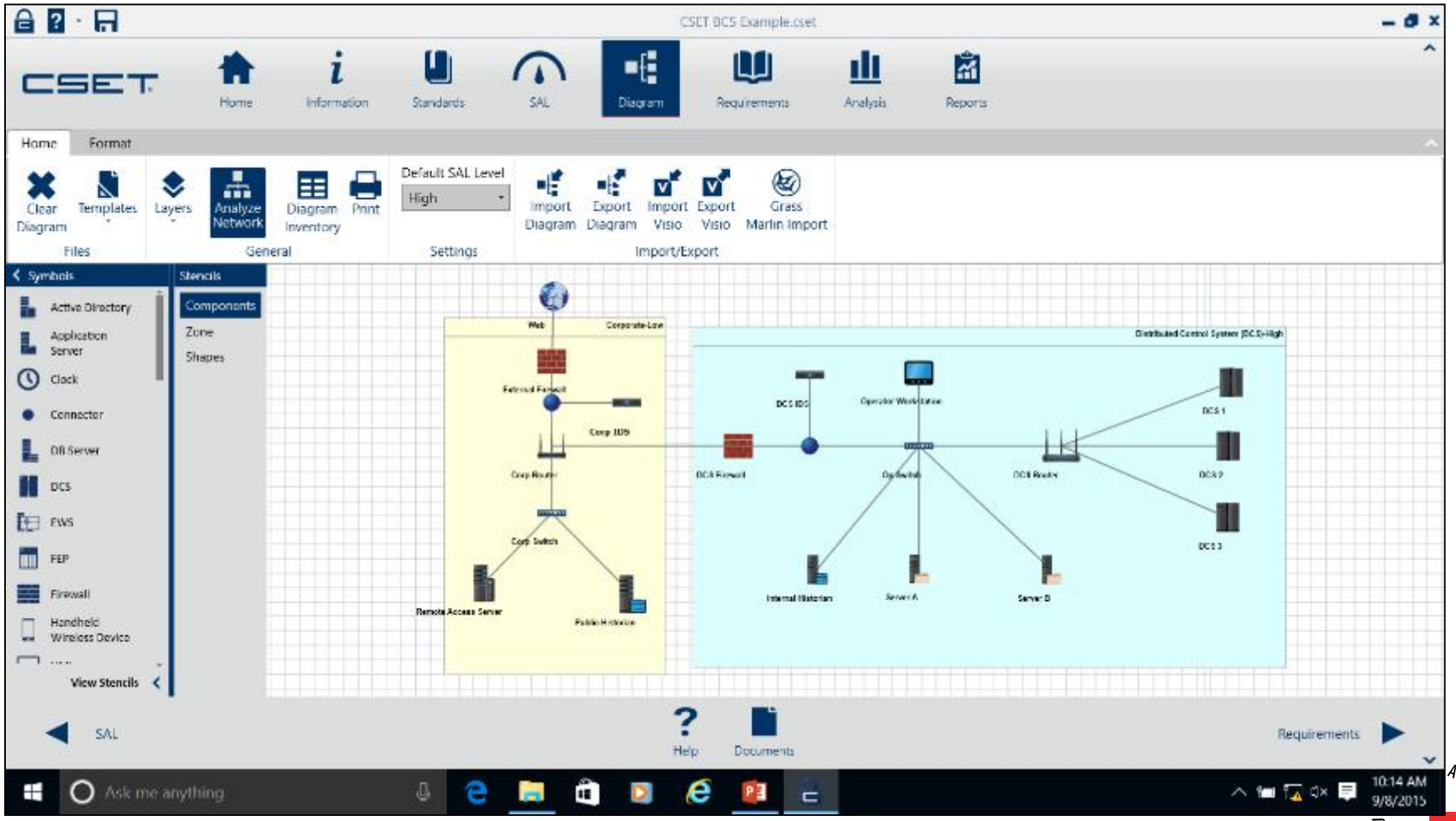


Select Standards → Determine Assurance Levels → Create Diagram → Answer Questions

	t Name
	-53 R3
	R3 App I
	-53 R4
	R4 App J
	800-82
	0-82 V1
	0-82 V2
	CAG
	ponents
	FATS
	SI 1253
	SSI ICS
	OR 7
	8500.2
	NGAA
	Key
	SF V1
	0809
NERC CIP-002 through CIP-009 Rev 3	NERC Rev 3
NERC CIP-002 through CIP-009 Rev 4	NERC Rev 4
NISTIR 7628 Guidelines for Smart Grid Cyber Security: Vol. 1	NISTIR 7628
NRC Regulatory Guide 5.71	NRC 5.71
TSA Pipeline Security Guidelines April 2011	TSA
Universal Questions Set	Universal

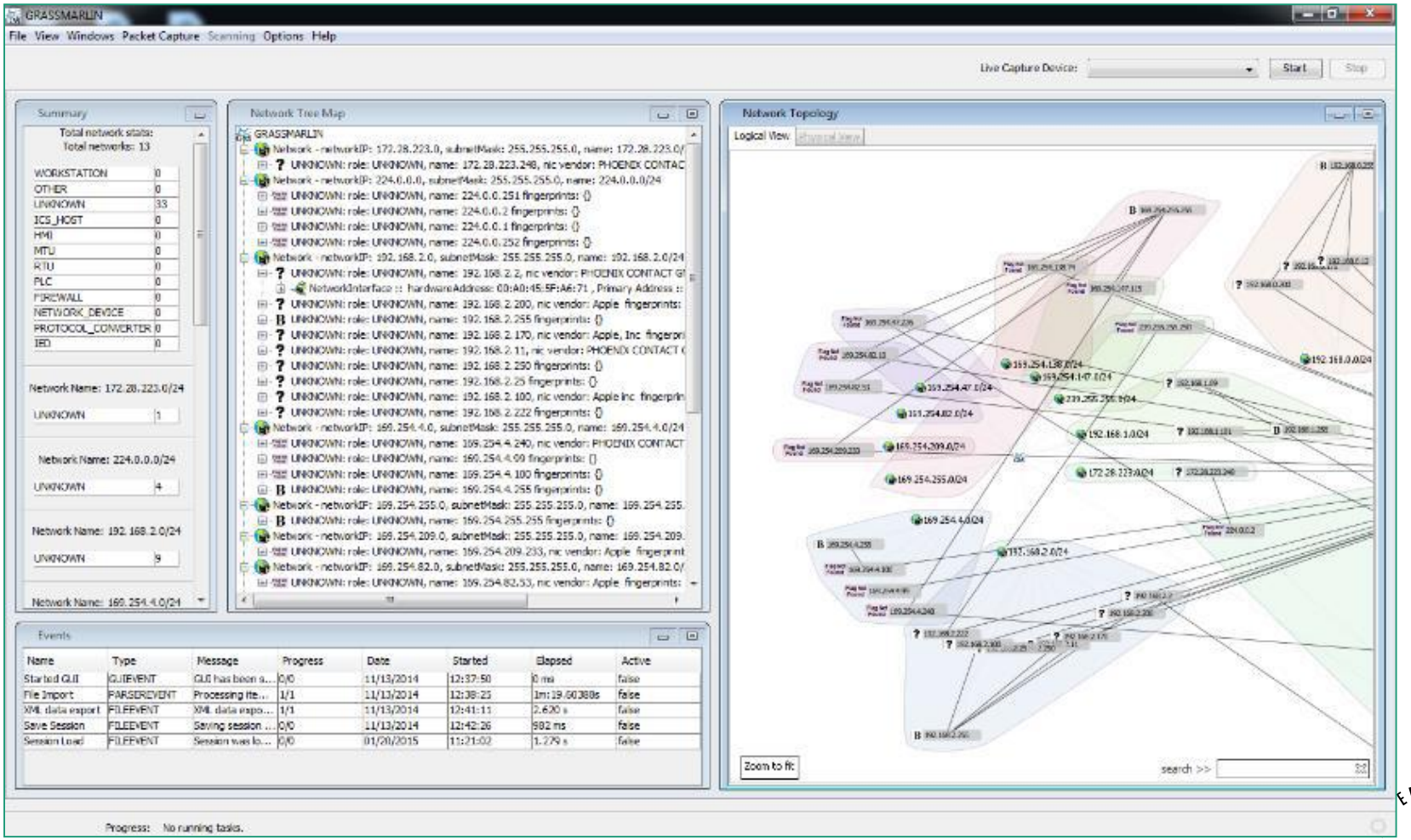
DoD Directing Standardized Assessments via CSET

CSET Diagram Tool Enhancements



Additional Components, Building Control System template…more to come!

GrassMarlin Passive Network Discovery Tool



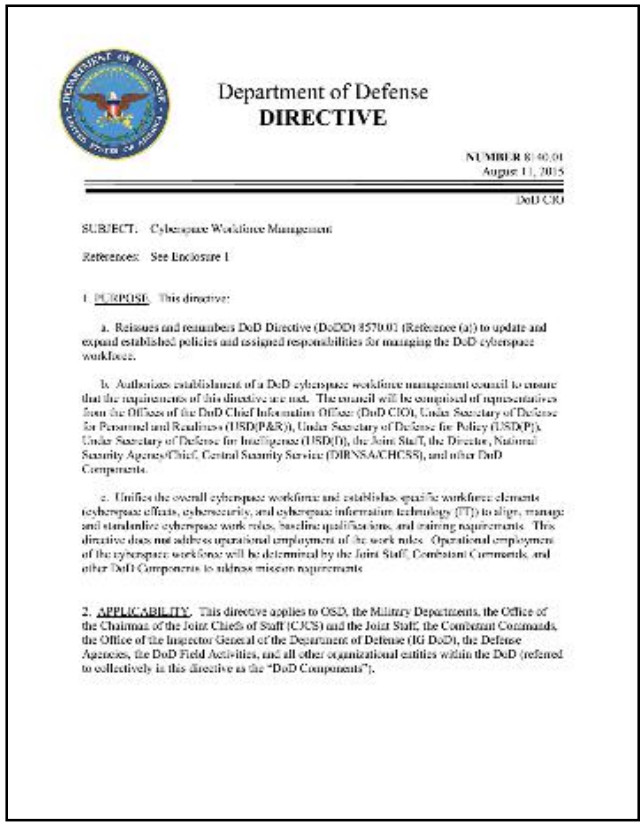
Working with other products to get Visio import templates, CSET Plug-in

Procurement Challenges

Initially likely to pay a premium, then becomes industry standard
LEED is a good corollary, took a few years….but now a green is gold

DoD 8140 – Cyberspace Workforce

DoDM 8570 changed to DoDD 8140 Cyberspace Workforce Management – AO's will need "Specialized Skills and Knowledge"



Department of Defense
DIRECTIVE

NUMBER 8140.01
August 11, 2015
DoD CIO

SUBJECT: Cyberspace Workforce Management

References: See Enclosure 1

1. PURPOSE. This directive:

a. Reissues and renumbers DoD Directive (DoDD) 8570.01 (Reference (a)) to update and expand established policies and assigned responsibilities for managing the DoD cyberspace workforce.

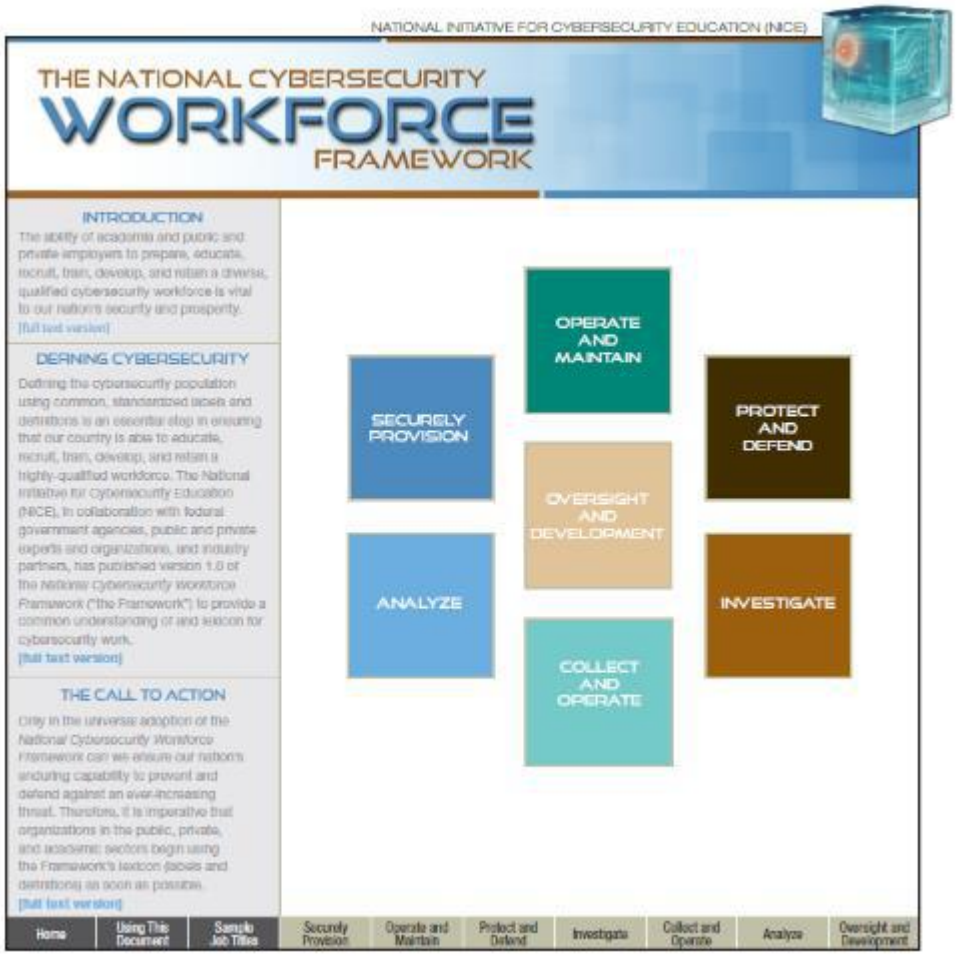
b. Authorizes establishment of a DoD cyberspace workforce management council to ensure that the requirements of this directive are met. The council will be comprised of representatives from the Offices of the DoD Chief Information Officer (DoD CIO), Under Secretary of Defense for Personnel and Readiness (USD(P&R)), Under Secretary of Defense for Policy (USD(P)), Under Secretary of Defense for Intelligence (USD(I)), the Joint Staff, the Director, National Security Agency/Chief, Central Security Service (DIRNSA/CHCSS), and other DoD Components.

c. Unifies the overall cyberspace workforce and establishes specific workforce elements (cyberspace effects, cybersecurity, and cyberspace information technology (IT)) to align, manage and standardize cyberspace work roles, baseline qualifications, and training requirements. This directive does not address operational employment of the work roles. Operational employment of the cyberspace workforce will be determined by the Joint Staff, Combatant Commands, and other DoD Components to address mission requirements.

2. APPLICABILITY. This directive applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff (CJCS) and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense (IG DoD), the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this directive as the "DoD Components").

Unifies the overall cyberspace workforce and establishes specific workforce elements (cyberspace effects, cybersecurity, and cyberspace information technology (IT)) to align, manage and standardize cyberspace work roles, baseline qualifications, and training requirements.

Workforce Cyber Skills – NIST NICE



Collect and Analyze Data Capture cybersecurity workforce and training data to understand capabilities and needs.

Recruit and Retain Incentivize the hiring and retention of highly skilled and adaptive professionals needed for a secure digital nation.

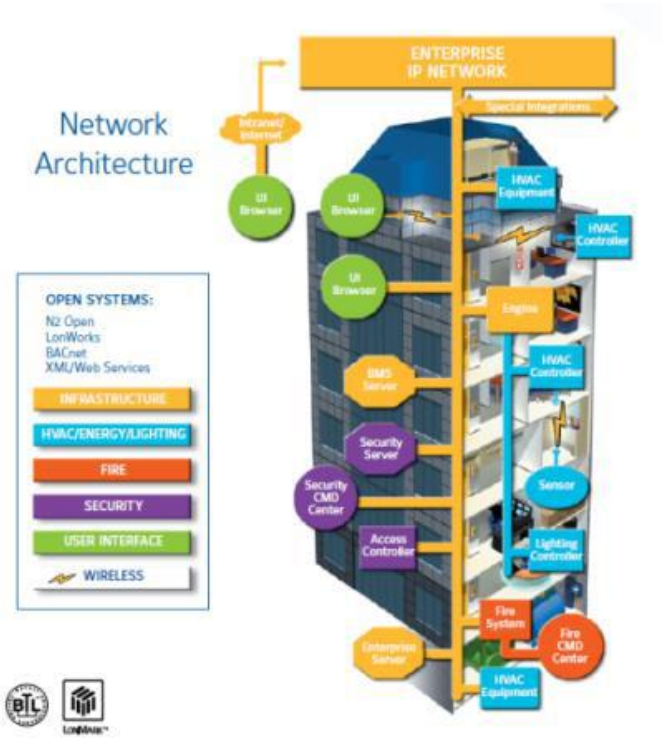
Educate, Train, and Develop Expand the pipeline for and deliberately develop an unrivaled cybersecurity workforce.

Engage Educate and energize all cybersecurity workforces and the American public to strengthen the nation's front lines of cybersecurity.

Workforce Cyber Skills – CS PIT

Operate and Maintain

- Data Administration
- Knowledge Management
- Customer Service and Technical Support
- Network Services
- System Administration
- Systems Security Analysis



Securely Provision

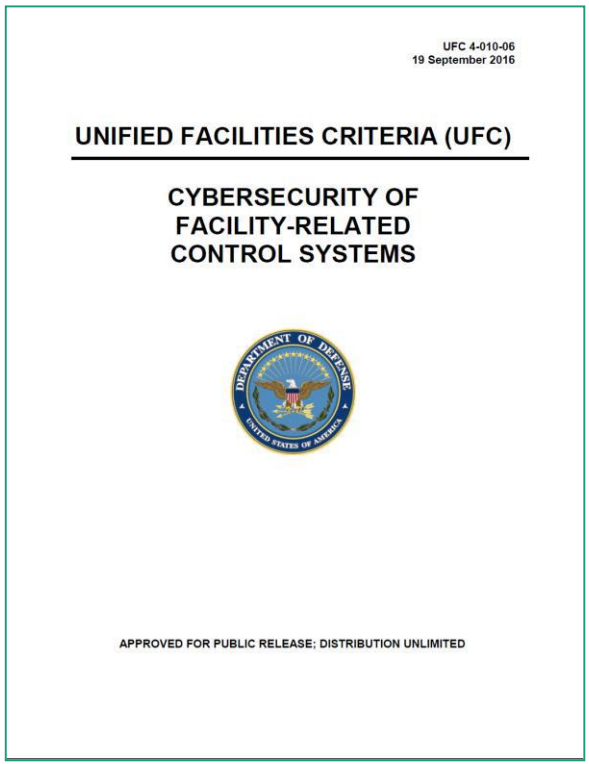
- Information Assurance (IA) Compliance
- Software Assurance and Security Engineering
- Systems Security Architecture
- Technology Research and Development
- Systems Requirements Planning
- Test and Evaluation
- Systems Development

Protect and Defend

- Computer Network Defense (CND) Analysis
- Incident Response
- Computer Network Defense (CND) Infrastructure Support
- Vulnerability Assessment and Management

UFC Facilities-Related Cybersecurity

Released Sep 2016



UFC 4-010-06
19 September 2016

UNIFIED FACILITIES CRITERIA (UFC)

CYBERSECURITY OF FACILITY-RELATED CONTROL SYSTEMS

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

3-1.1 Five Steps for Cybersecurity Design

The five steps for cybersecurity design are:

Step 1: Based on the organizational mission and details of the control system, the System Owner and Authorizing Official determine the confidentiality, integrity, and availability impact levels (LOW, MODERATE, or HIGH) for the control system.

Step 2: Use the impact levels to select the proper list of controls from NIST SP 800-82.

Step 3: Using the DoD master Control Correlation Identifier (CCI) list, create a list of relevant CCIs based on the controls selected in Step 2.

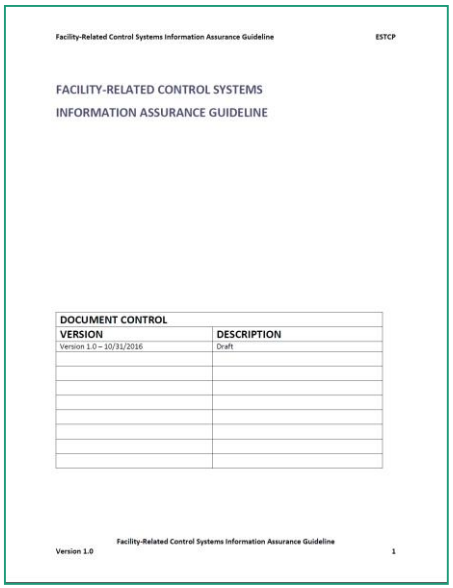
Step 4: Categorize CCIs and identify CCIs that require input from the designer or are the designer's responsibility.

Step 5: Include cybersecurity requirements in the specifications and provide input to others as required.

Any organization can use the UFC for their CS

http://www.wbdg.org/ffc/dod/unified-facilities-criteria-ufc/ufc-4-010-06

Information Assurance Guideline For Facility-Related CS


Facility-Related Control Systems Information Assurance Guideline ESTCP

FACILITY-RELATED CONTROL SYSTEMS
INFORMATION ASSURANCE GUIDELINE

DOCUMENT CONTROL

VERSION	DESCRIPTION
Version 1.0 – 10/31/2016	Draft

Facility-Related Control Systems Information Assurance Guideline
Version 1.0 1

The IA Guideline has several key sections that establish new RMF contractual and deliverable requirements:

- Hybrid/Converged CS
- Project Roles and Responsibilities
- **Requirements For Subject Matter Experts**
- **Test And Development Environment and Tools**
- Required Submittals
- Applicable ESTCP CS Templates (FAT & SAT, PenTest)
- Typical Sequence Of CS Design And Construction Activities

Any organization can use for their CS

https://www.serdp-estcp.org/Investigator-Resources/ESTCP Resources/Demonstration-Plans/Cybersecurity-Guidelines

Information Assurance Guideline For Facility-Related CS – Subject Matter Experts

Control Systems Cybersecurity Specialist: The Control Systems Cybersecurity specialist shall have a minimum of five years' experience in control system network and security design and shall maintain current certification as a Global Industrial Cyber Security Professional (GISCP) or Certified Information Systems Security Professional (CISSP).

Information and Communication Technology Specialist: The Information and Communication Technology specialist shall have a minimum of five years' experience in control system network and security design and shall maintain current certification as a Registered Communications Distribution Designer (RCDD®).

System Integration Specialist: The System Integration specialist shall have a minimum of five years' experience in control system network and shall maintain current certification as a Certified System Integrator (CSI) for the products they are integrating and/or be Control System Integrators Association (CISA) Certified.

Information Assurance Guideline For Facility-Related CS – Test And Development Environment

For new or major modernization projects, the Systems Integrator will **establish a Test and Development Environment (TDE) that replicates the Production Environment to the highest degree possible starting with the Level 4 Workstations, Servers, software and with at least one of each of the Level 3-0 major components, devices, and actuators.** At approximately the 50-75% construction complete, the TDE will be used to perform Factory Acceptance Testing (FAT) of the project to ensure the project has end-to-end functionality, has been properly configured using the Security Content Automation Protocol (SCAP) tool and the Security Technical Implementation Guides (STIGS), all patches (OS and CS) are installed and properly configured, and begin creating the artifacts for the draft System Security Plan.

At approximately 95-100% construction complete, the TDE will be used to conduct Site Acceptance Testing of the complete CS, and if required, Penetration testing. **The SAT artifacts will be included in the final System Security Plan, FMC and Jump-Kit (if required).**

Information Assurance Guideline For Facility-Related CS – TTP Requirements

1.5 REQUIRED SUBMITTALS

The Contractor(s) shall develop and upload into the DoD CIO eMASS tool, all required artifacts and supporting documentation. This effort should result in the creation of an Authority To Operate (ATO) package. The required artifacts are determined by the system security classification, system categorization, and cybersecurity controls. This information may include but is not limited to the list below:

a. System Security Plan (SSP)
b. Configuration Management Plan (CMP)
c. Disaster Recovery Plan (DRP)
d. Continuity of Operations (COP)
e. Information Technology Contingency Plan (ITCP)
f. Incidence Response Plan (IRP)
g. Security Assessment Report (SAR)
h. Plan of Action and Milestones (POAM)
i. System Architecture/Topology/Data Flow
j. Configuration Validation Checklist
k. Security Classification Guide
l. System Configuration Guide
m. Hardware Inventory List
n. Software Inventory List
o. Physical Security Plan
p. Personnel Security Plan
q. Information Assurance Vulnerability Management (IAVM) Process
r. Patch Management Process, Connection Approval / System Approval documentation
s. Ports, Protocols, and Services (PPS) List
t. Active Directory (AD) Documentation, (if applicable)
u. Jump-Kit Rescue CD

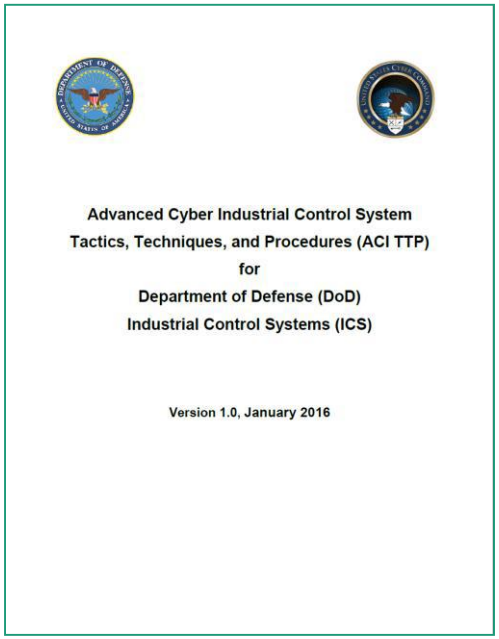
Utility Monitoring and Control System Engineering Requirements Manual — **Navy Medicine West**

(Both hardware and software/firmware lists should also include Common Criteria EAL status, DADMS entry number, and OS/IOS/Firmware version(s) as applicable).

- Network diagram
  - Network diagram must show equipment locations, names, models, and IP addresses on network communications schematic.
- Jump-Kit Rescue CD
  - The Rescue CD is a bootable CD with tools, rootkit detection, master boot record check, and other capabilities. 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. The Jump-Kits must be maintained and be a part of configuration management. When configuration files or new versions of operating systems or applications are updated, the Jump-Kits need to be updated as well.

TTP Jump-Kit Rescue CD/DVD

ACT 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 (DCS),** 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.**

Any organization can use the TTP's for any IT and/or OT

http://www.wbdg.org/files/pdfs/jbasics_aci_ttp_2016.pdf

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)

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

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.

Baselining and Routine Monitoring

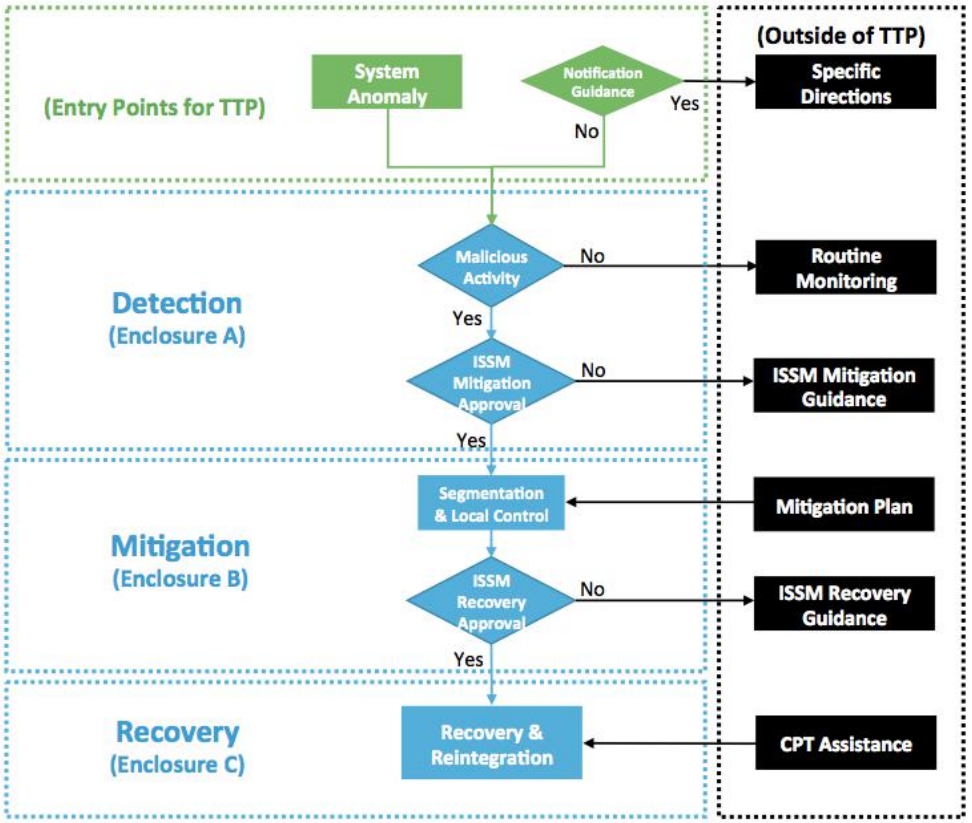
Before the ACI TTP are adopted, ICS and IT managers should establish what a FMC network is as it pertains to their specific installations and missions. The ACI TTP defines FMC as a functional recovery point for both the ICS and the SCADA. Once this is defined, ICS and IT managers should capture the FMC condition of their network entry points (e.g., firewalls, routers, remote access terminals, wireless access points, etc.), network topology, network data flow, and machine/device configurations, then store these in a secure location. **This information should be kept under configuration management and updated every time changes are made to the network.** This information forms the FMC baseline. ***The FMC baseline is used to determine normal operational conditions versus anomalous conditions of the ICS.***

FMC = Fully Mission Capable

Detection, Mitigation, Recovery Overview

Navigating Detection, Mitigation, and Recovery Procedures

Detection, Mitigation, and Recovery Procedures are contained within enclosures A through C. **While Detection Procedures lead to Mitigation Procedures, and Mitigation Procedures lead to Recovery Procedures, each enclosure can also be executed as a stand-alone resource as well as be incorporated into local procedures.** The following is an overview for navigating the Detection, Mitigation, and Recovery portions of the TTP.



DETECTION PROCEDURES SERVER EXAMPLE

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: 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: 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

A.2.3 Server/Workstation: Irregular Process Found

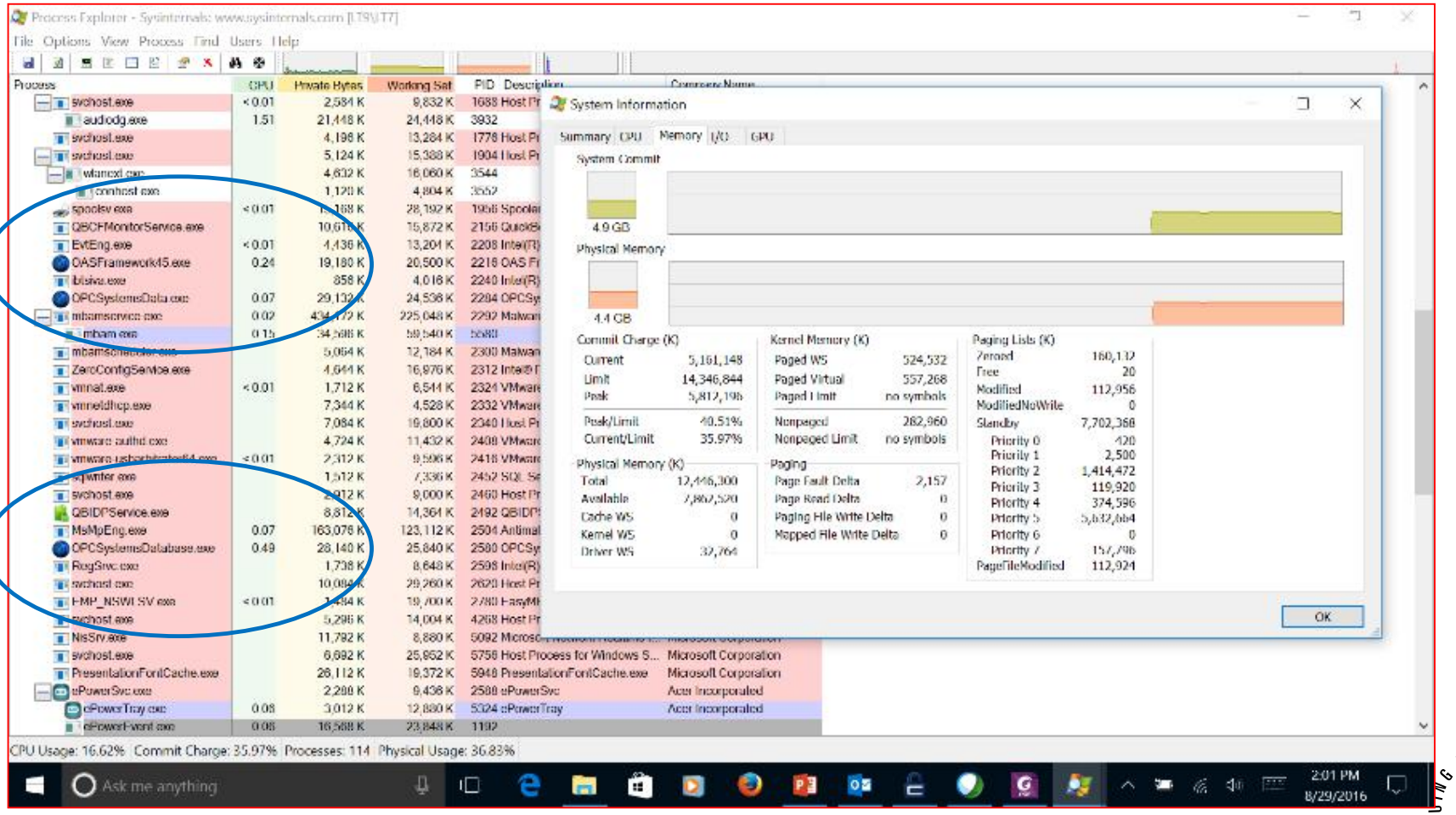
- **Functional Area:** IT or ICS
- **Description:** On any computer-based server, workstation, including SCADA equipment, an irregular process was found

Step	Procedures
Investigation	1. **DETERMINE** if the new process belongs to an authorized installation: 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	2. If the new process belongs to an authorized installation: 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 *Routine Monitoring*.
If Action Required	3. If the new process **does not** belong to an authorized installation: a. **DOCUMENT** in Security Log. b. **GO TO** Section *A.3, A.3.1 Integrity Checks Table.* (See recommended checks below.) **LOCATE** the integrity check associated with server or workstation you are investigating and **EXECUTE** the Integrity checks. **Recommended Checks:** A.3.2.1 Server/Workstation Process Check A.3.2.2 Server/Workstation Log Review A.3.2.4 Server/Workstation Communications Check A.3.2.16 Peripherals Integrity Check A.3.2.9 Controller Integrity Check A.3.2.13 Server/Workstation Rootkit Check 4. Once you have completed all appropriate Integrity Checks, **GO TO** section ***A.2.29 Action Step***.

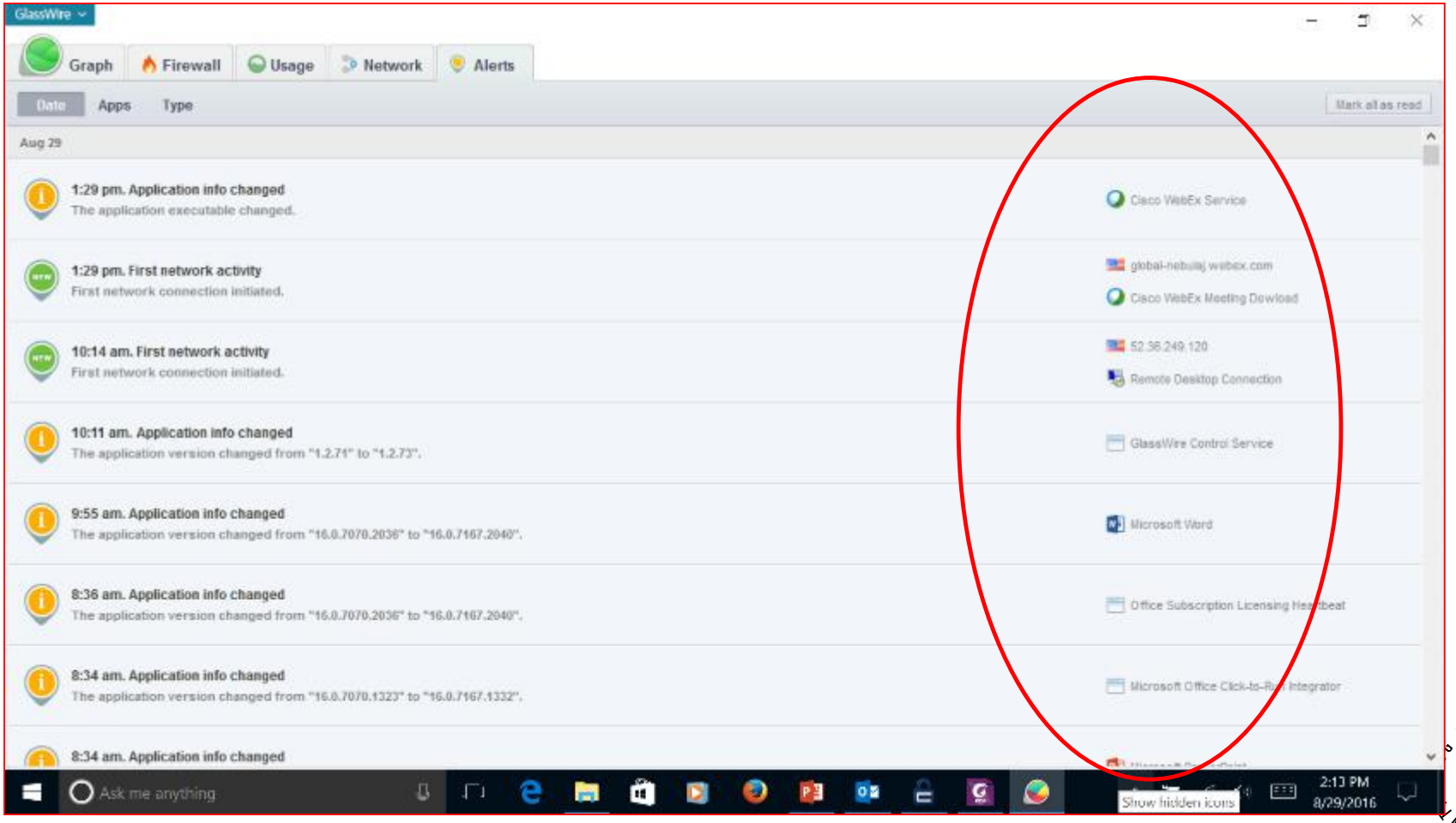
DETECTION PROCEDURES SERVER EXAMPLE

A.3.2.1 Server/Workstation Process Check	
• **Who should do this check:** The organization or individual responsible for the server or workstation • **What is needed for this check:** 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.	If the machine is **responsive**, **EXECUTE** steps a and b below. Once completed, **RETURN** to this section, and resume with Step 2. a. Section: A.3.2.2 Server/Workstation Log Review. b. Section: A.3.2.3 Unauthorized User Account Activity. If the machine is **not responsive**, **GO TO** Section *A.3.2.5 Server/Workstation Unresponsive Check*.
2.	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.
3.	**Process Check: LAUNCH** SysInternals: **CHECK** for processes that do not appear legitimate. This can include (but is not limited to) processes that: 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.	If an anomalous process was found: a. **DOCUMENT** details of the event in Security Log. b. **CONTACT** system administrator responsible for the machine or the command ISSM. (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.	If an anomalous process was not found: a. **DOCUMENT** the **Severity Level as None (0)**. b. **RETURN** to the previous diagnostic procedure and continue with *Recommended Checks*.

DETECTION PROCEDURES SERVER EXAMPLE SYSINTERNALS



DETECTION PROCEDURES SERVER EXAMPLE GLASSWIRE



Chapter 3 – Mitigation Concepts

Cyber Incident Analysis - It is important to note that **Mitigation actions can very easily destroy information or forensic evidence that could be useful in follow-on technical analysis of an incident.** As such, it may become necessary to conduct Mitigation Procedures without performing technical analysis to keep the system operational.

Cyber Incident Response - Organizations must be prepared in advance for any Mitigation. Decisions made in haste while responding to a critical incident could lead to further unintended consequences. Therefore, **Mitigation Procedures, tools, defined interfaces, and communications channels and mechanisms should be in place and previously tested.**

Mitigation Course of Action (COA) -**Develop a plan that lists the specific Mitigation steps to take and which identifies the personnel by job description that should take those steps.** In this way, when an incident does occur, appropriate personnel will know how to respond. Escalation procedures and criteria must also be in place to ensure effective management engagement during Mitigation actions. **Organizations must define acceptable risks for incident containment and develop strategies and procedures accordingly.** This should be conducted during annual risk management activities.

Chapter 4 – Recovery Concepts

a. **The Recovery phase begins once the system under attack has been stabilized and infected equipment has been isolated from the network.** Recovery of the systems will require the use of the resources located in the Jump-Kit, the IT and CS system schematics, and the wiring and logic diagrams, and may require vendor assistance. Successful Recovery of the CS system after the cyber incident will depend upon the technical knowledge and skills of the CS and IT operators and will require a high level of communication and consultation between these team members and with the ISSM.

b. **Because of the wide variance in ICS/SCADA system design and applications, these Recovery Procedures are not specific to a particular make or model of equipment** but are general in terms of application.

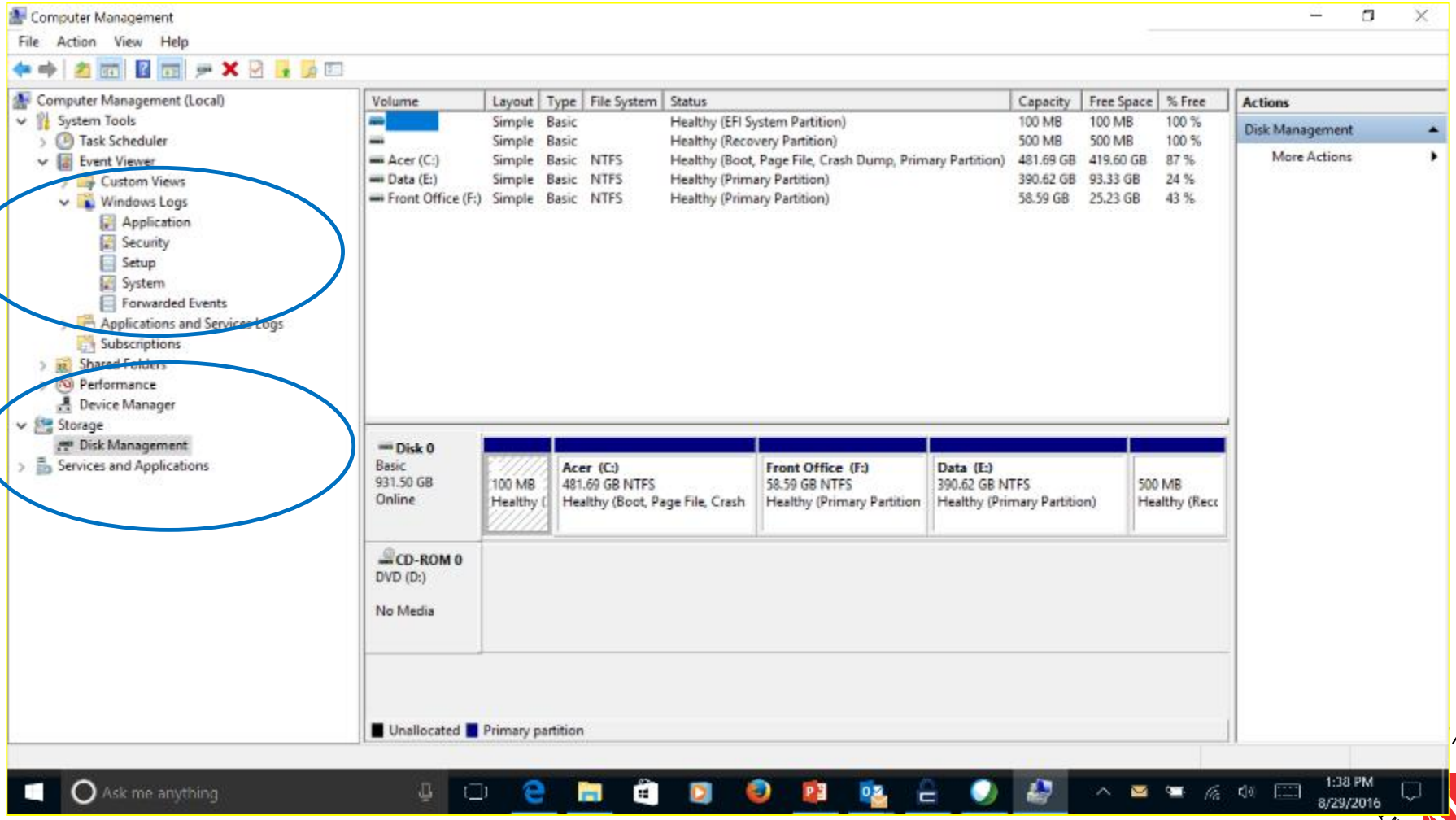
RECOVERY PROCEDURES SERVER EXAMPLE

Typical Equipment: Servers/Workstations	
• **Who should perform this procedure:** The organization or individual who has knowledge of the network configuration and the operation of the ICS end process • **What is needed for this procedure:** FMC baseline topology and Jump-Kit	
Step	**Recovery Procedure**
1.	**RECORD** all steps taken while performing these procedures. These records are a requirement of CJCSM 6510-01B and will be utilized for forensic analysis of the cyber incident.
2.	**MAINTAIN** primary power (if possible) to the server/workstation until an image can be saved of the server/workstation memory. **SAVE** an image of the drive(s) and volatile memory (if possible and unless otherwise directed) for forensic analysis. This may require a reboot. First capture volatile memory, and then **MAKE** an image of the drive.
3.	**REMOVE and REPLACE** the affected server/workstation. Device replacement will preserve the server/workstation nonvolatile memory for forensic evidence of the cyber incident.
4.	**If** a replacement server/workstation is not available, **REPLACE** the hard drive with a known, good back-up drive containing known, good software.
5.	**DO NOT REIMAGE** any devices unless authorized by the CPT and/or the ISSM. Reimaging the affected server/workstation drive(s) will destroy forensic evidence of the cyber incident. **If** a replacement server/workstation or hard drive is not available, **REIMAGE** the affected server/workstation from a trusted, known good back-up source.
6.	**VERIFY** that the latest vendor operating system, software, and firmware patches are installed on the server/workstation. **INSTALL** updates as required.
7.	**UPDATE** passwords on server/workstation. **UTILIZE** robust passwords.

ENCLOSURE D: MONITORING PROCEDURES

Routine Monitoring: Computer Assets	
• Functional Area: IT or ICS • What you need to perform this procedure: 1. From the FMC Baseline Documents binder, extract FMC Data Flow Diagram and User Accounts Table for the assets being monitored 2. From the FMC Baseline Documents binder, extract FMC Topology Diagram 3. For 2nd Stage Monitoring, Baseline CD-r or digital versatile disc (DVD)-r from Jump-Kit 4. Administrator rights	
Step	**Computer Assets Procedures**
1.	**MAKE** a copy of the *FMC Data Flow Diagram, User Account* Table, and the *FMC Topology Diagram,* and **RETURN** the originals to the *FMC Baseline Documents* binder.
2.	**LOG** on to asset, and run as "administrator".
3.a	**DISPLAY** Security Log – **Windows XP**: a. Open Computer Management. b. In the console tree, click **Event Viewer**. **Where?** System Tools > Event Viewer c. In the details pane, double-click **Security**.
3.b.	**DISPLAY** Security Log - **Windows 7 and higher**: a. To open Event Viewer, click **Start**, click **Control Panel**, click **System and Maintenance**, double-click **Administrative Tools**, and then double-click **Event Viewer**. b. **OPEN** Event Viewer. c. In the console tree, open **Global Logs**, and then click **Security**. The results pane lists individual security events.
4.	**REVIEW** Security Logs since last *Routine Monitoring* check for the following user actions: a. Unauthorized user logging in. b. Rapid and/or continuous log-ins/log-outs. c. Users logging into accounts outside of normal working hours and for no apparent reason. d. Numerous failed log-in attempts found in logs on administrator accounts or other user accounts. e. User accounts attempting to escalate account privileges or access areas or assets not required by their jobs. f. Logs that have been erased or appear altered (look for missing days or times).

ENCLOSURE D: MONITORING PROCEDURES WINDOWS LOGS AND DISK MANAGER



ENCLOSURE G: DATA COLLECTION FOR FORENSICS

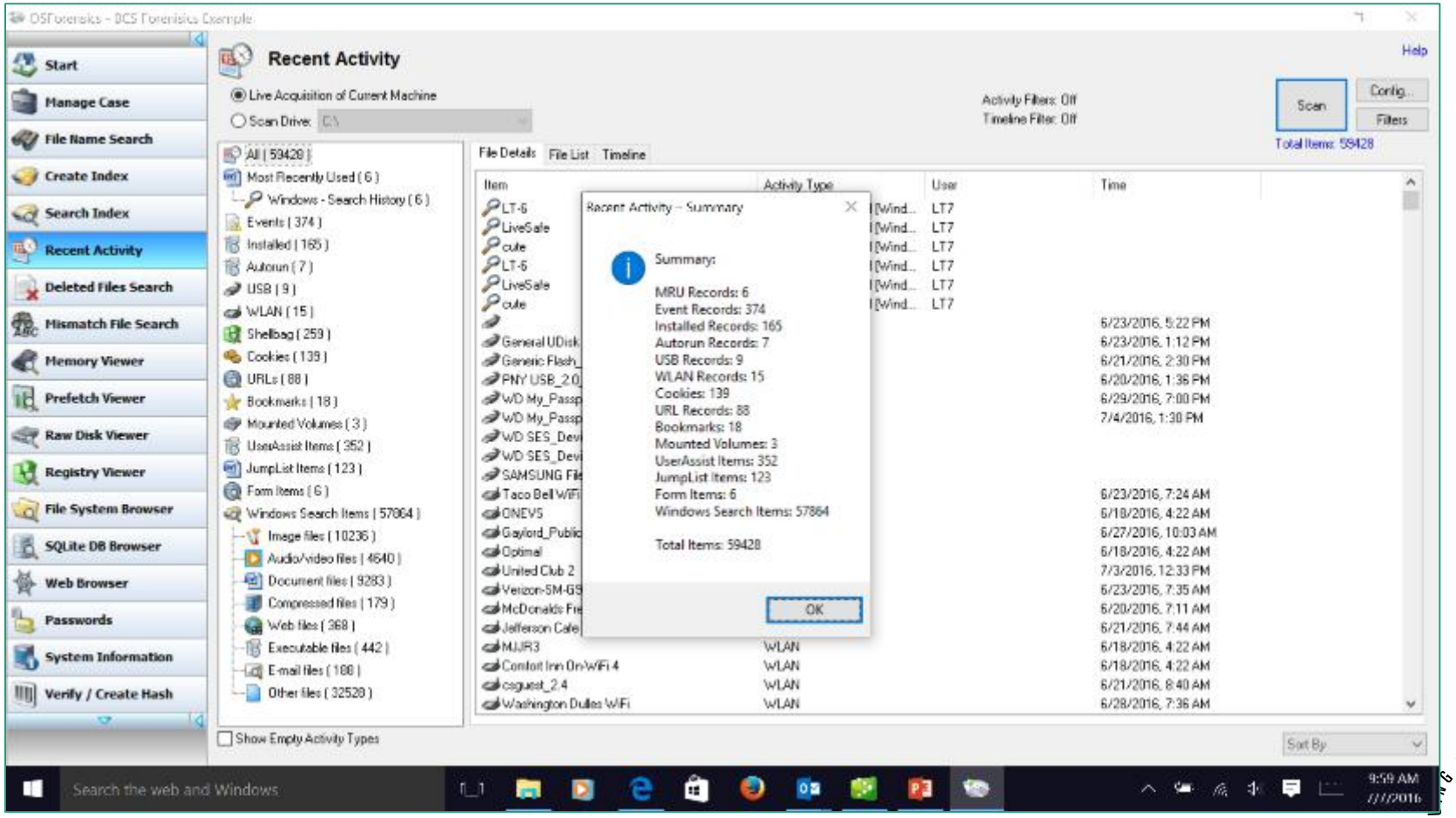
G.1. Data Collection for Forensics Introduction

a. Description. Data collection for forensics involves the acquisition of volatile and nonvolatile data from a host, a network device, and ICS field controllers. Memory acquisition involves copying the contents for volatile memory to transportable, non-volatile storage. Data acquisition is copying non-volatile data stored on any form of media to transportable, non-volatile storage. **A digital investigator seeks to preserve the state of the digital environment in a manner that allows the investigator to reach reliable inferences through analysis. (**Ligh, 2014)

G.2. Documentation of Data Collection

a. **It is important to document environmental observations of what the device is doing, its symptoms and anomalies, and if the device is currently running or shut down.** It is also important to note who has had access to the device and what the person did—if any actions were taken. Also include documents for each step that is taken while acquiring data for forensics.

OS Forensics Recent Activity



Reporting Incidents to CERT

https://www.us-cert.gov/NCCIC-Cyber-Incident-Scoring-System

Reporting Incidents to CERT

Follow the steps below to send an incident notification to US-CERT:

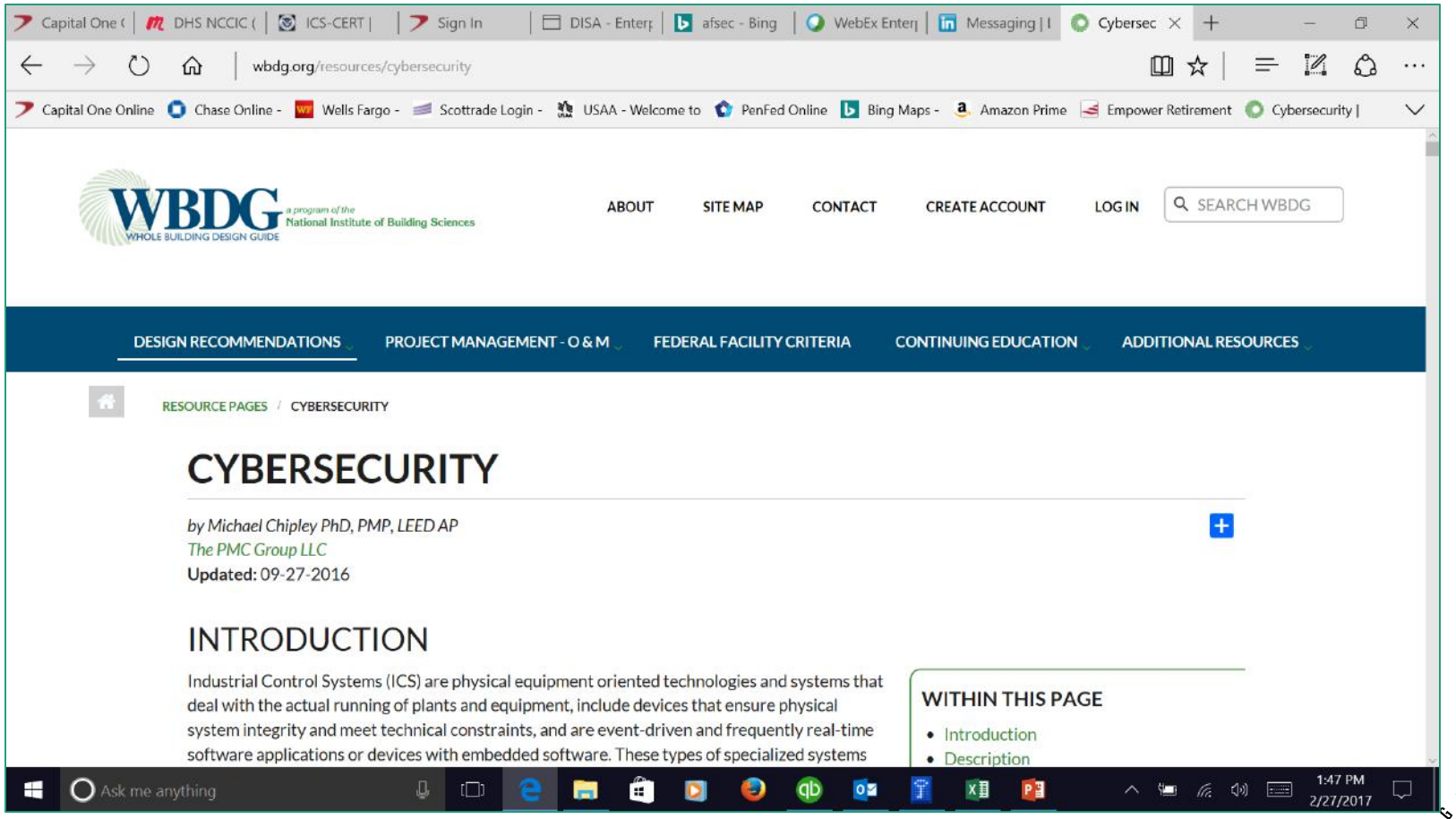
1. Identify functional impact (see Impact Classification table) ***required**
2. Identify information impact (see Impact Classification table) ***required**
3. Identify impact to recoverability (see Impact Classification table) ***required**
4. Identify threat vector (see Cause Analysis flowchart), if possible
5. Provide any mitigation details, if possible
6. Provide contact information and any available incident details ***required**

Incident Attributes

The following incident attribute definitions are taken from the NCISS.

Attribute Category	Attribute Definitions
Location of Observed Activity: Where the observed activity was detected in the network.	LEVEL 1 – BUSINESS DEMILITERIZED ZONE – Activity was observed in the business network's demilitarized zone (DMZ)
	LEVEL 2 – BUSINESS NETWORK – Activity was observed in the business or corporate network of the victim. These systems would be corporate user workstations, application servers, and other non-core management systems.
	LEVEL 3 – BUSINESS NETWORK MANAGEMENT – Activity was observed in business network management systems such as administrative user workstations, active directory servers, or other trust stores.
	LEVEL 4 – CRITICAL SYSTEM DMZ – Activity was observed in the DMZ that exists between the business network and a critical system network. These systems may be internally facing services such as SharePoint sites, financial systems, or relay "jump" boxes into more critical systems.
	LEVEL 5 – CRITICAL SYSTEM MANAGEMENT – Activity was observed in high-level critical systems management such as human-machine interfaces (HMIs) in industrial control systems.

WBDG Cybersecurity Resource Page



http://www.wbdg.org/resources/cybersecurity.php

This concludes The American Institute of Architects
Continuing Education Systems Course

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

Eric Nickel
Director Technical Solutions
Cell: 703-589-7849
E-mail: enickel@chinooksystems.com>

Daryl Haegley
President, DRH Consulting
Cell:
E-mail: dhaegley@gmail.com