The PMC Group LLC

Engineering a better tomorrow today

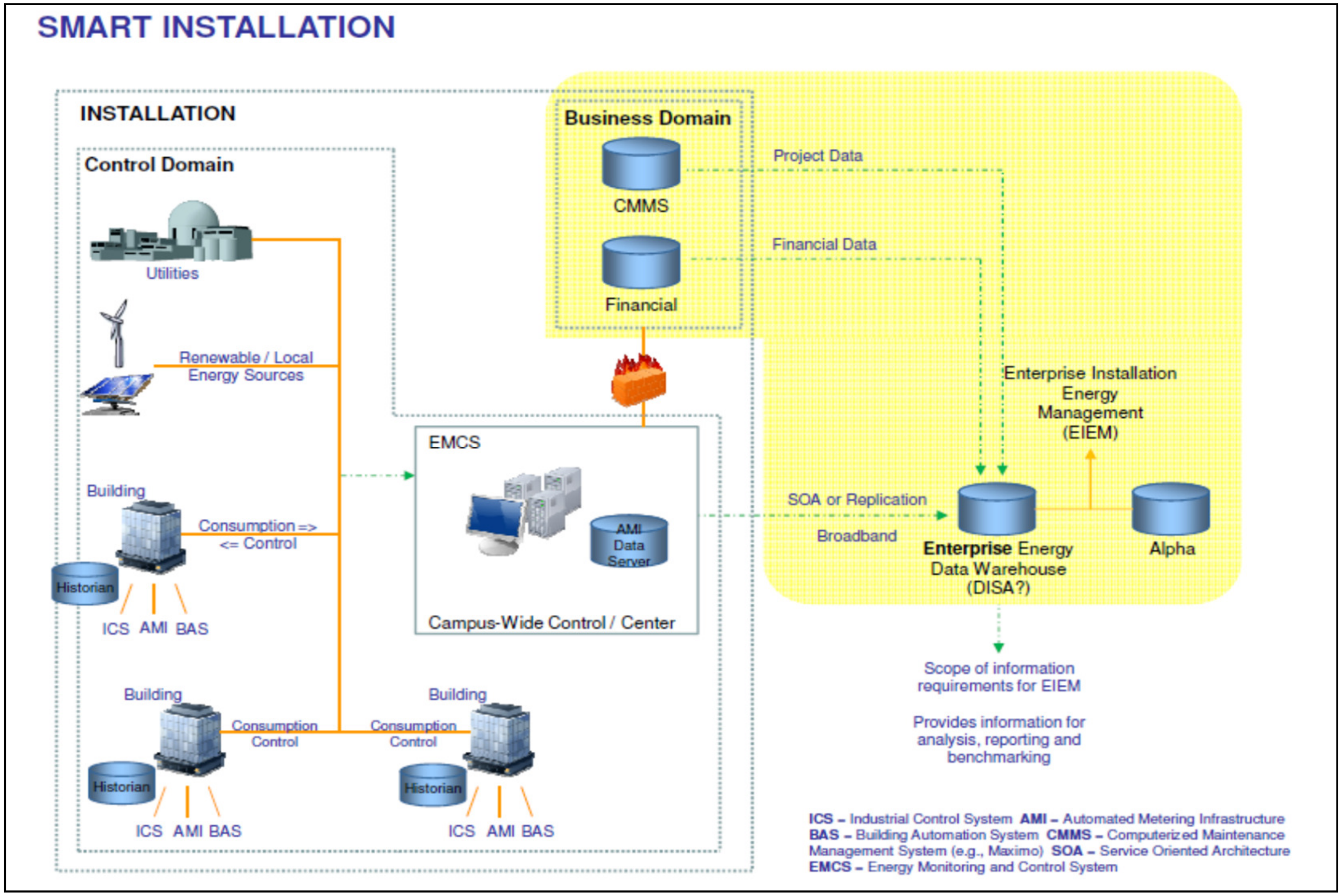
DoD Advanced Control Systems Tactics, Techniques and Procedures

Michael Chipley, PhD GICSP PMP LEED AP
President

Daryl Haegley, OCP CCO
DRH Consulting

September 14, 2016

In the Beginning….2010 Smart Installations



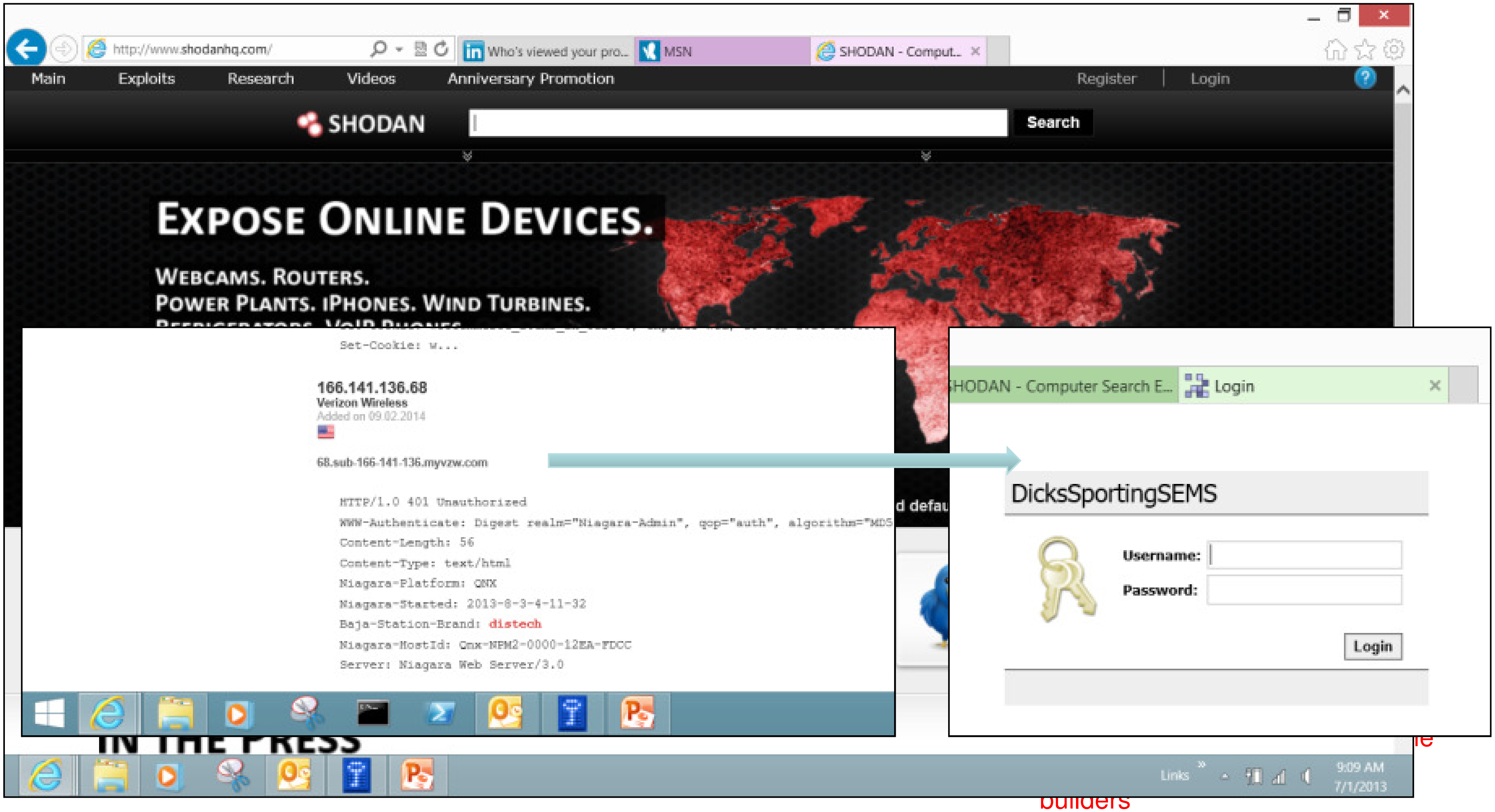
Scope of information requirements for EIEM

Provides information for analysis, reporting and benchmarking

ICS – Industrial Control System **AMI** – Automated Metering Infrastructure **BAS** – Building Automation System **CMMS** – Computerized Maintenance Management System (e.g., Maximo) **SOA** – Service Oriented Architecture **EMCS** – Energy Monitoring and Control System

A great idea rudely interrupted by reality…CIO AMI ATO denial,… and Stuxnet attack on Iranian Centrifuges

Shodan Site = Locates CS



```
Set-Cookie: w...
```

166.141.136.68
Verizon Wireless
Added on 09.02.2014

68.sub-166-141-136.myvzw.com

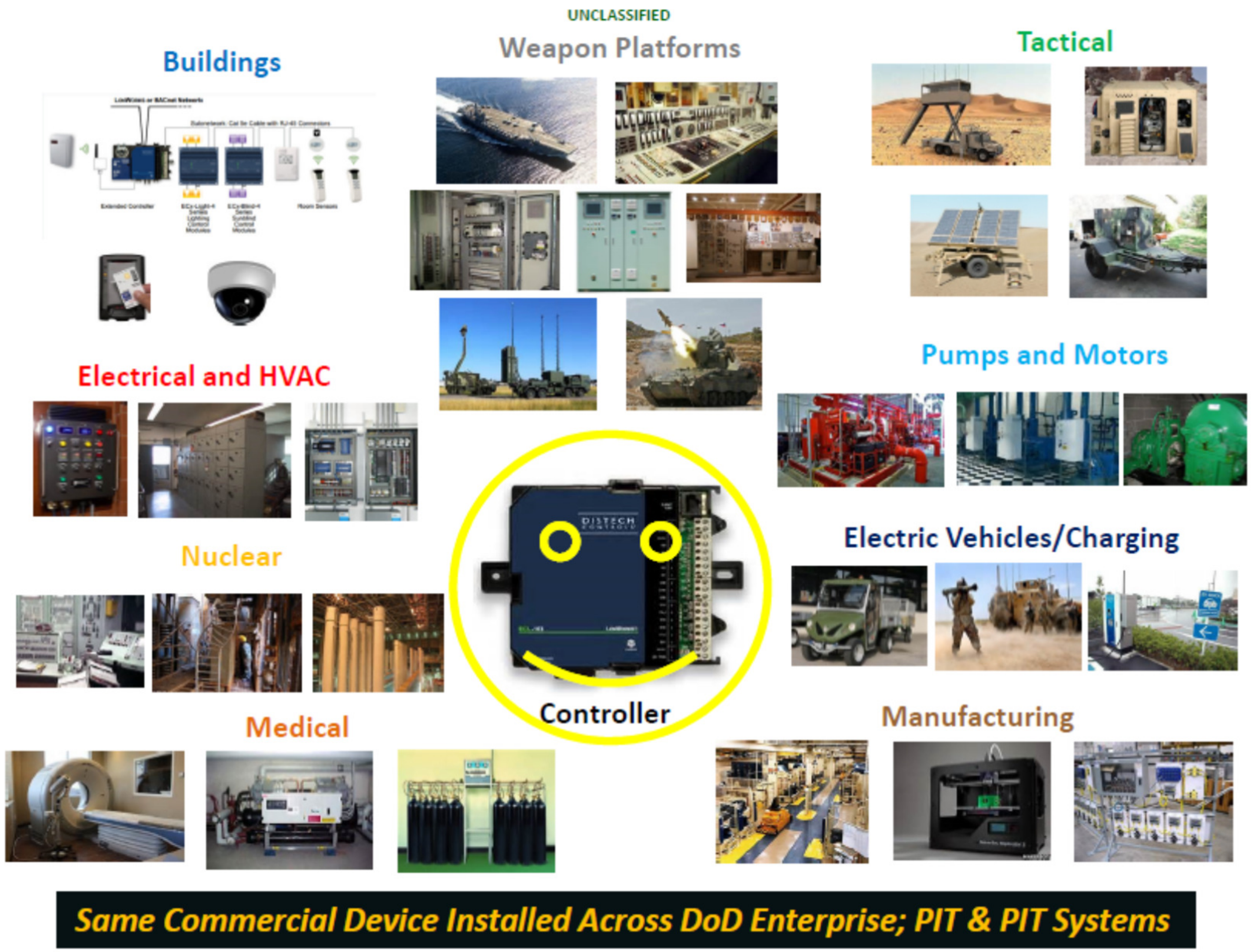
```
HTTP/1.0 401 Unauthorized
WWW-Authenticate: Digest realm="Niagara-Admin", qop="auth", algorithm="MD5
Content-Length: 56
Content-Type: text/html
Niagara-Platform: QNX
Niagara-Started: 2013-8-3-4-11-32
Baja-Station-Brand: distech
Niagara-HostId: Qnx-NPM2-0000-12EA-FDCC
Server: Niagara Web Server/3.0
```

DicksSportingSEMS

builders

DoD has many CS systems directly connected to internet with no protection, http

OT IP Controllers are in Everything



UNCLASSIFIED

Buildings

Weapon Platforms

Tactical

Electrical and HVAC

Pumps and Motors

Nuclear

Controller

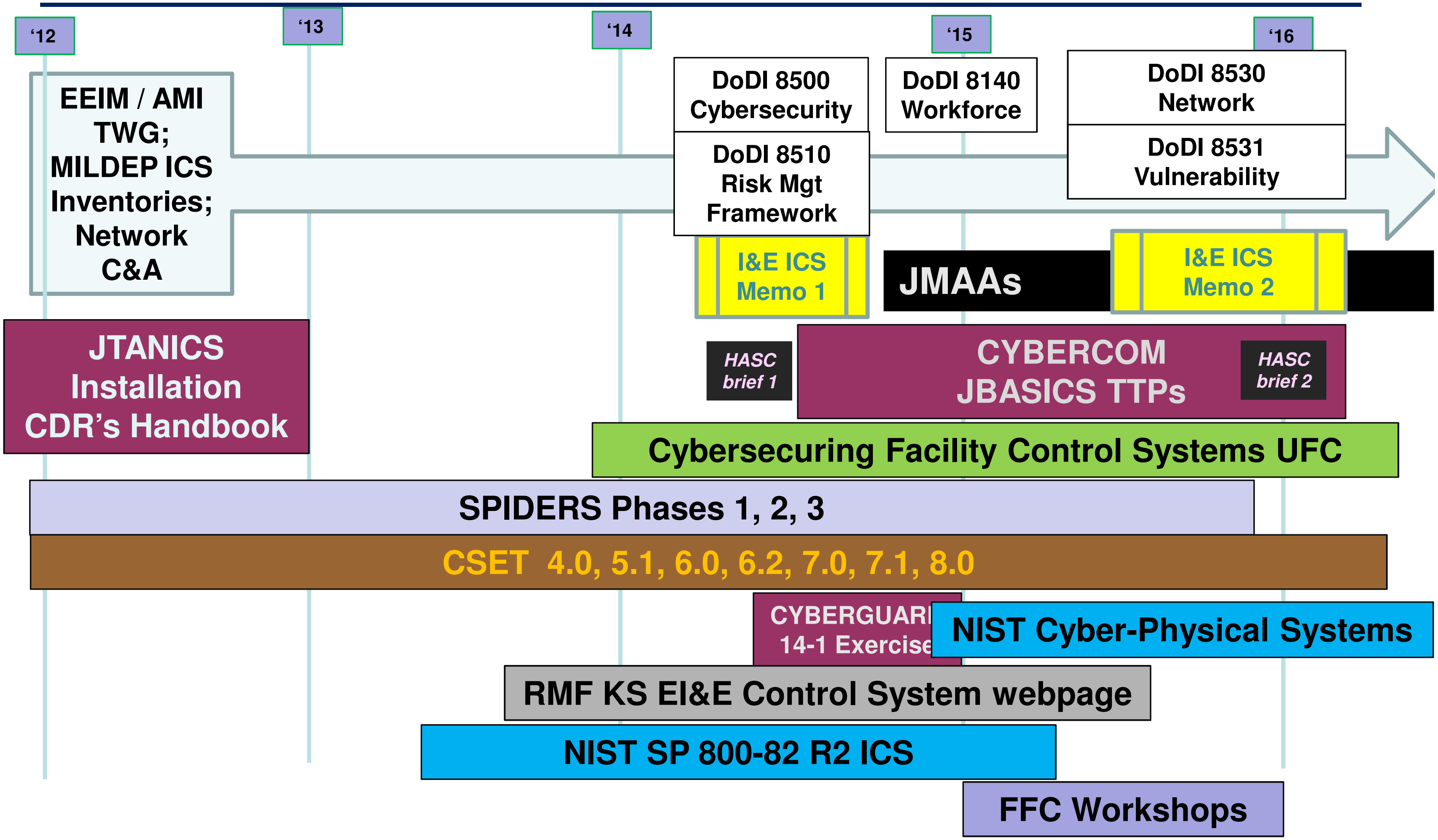
Electric Vehicles/Charging

Medical

Manufacturing

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

Broader Cybersecurity Efforts



‘12

‘13

‘14

‘15

‘16

EEIM / AMI TWG; MILDEP ICS Inventories; Network C&A

DoDI 8500 Cybersecurity

DoDI 8510 Risk Mgt Framework

DoDI 8140 Workforce

DoDI 8530 Network

DoDI 8531 Vulnerability

I&E ICS Memo 1

JMAAs

I&E ICS Memo 2

JTANICS Installation CDR’s Handbook

HASC brief 1

CYBERCOM JBASICS TTPs

HASC brief 2

Cybersecuring Facility Control Systems UFC

SPIDERS Phases 1, 2, 3

CSET 4.0, 5.1, 6.0, 6.2, 7.0, 7.1, 8.0

CYBERGUARI 14-1 Exercise

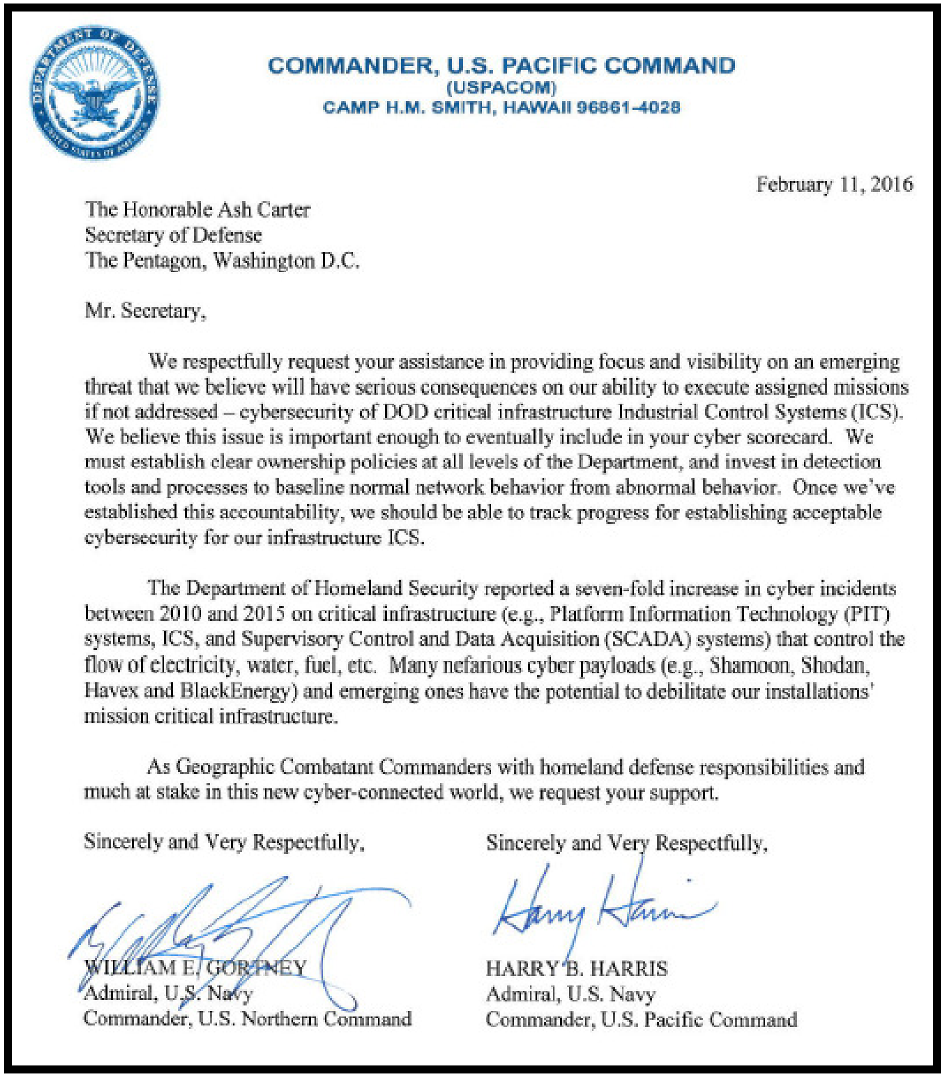
NIST Cyber-Physical Systems

RMF KS EI&E Control System webpage

NIST SP 800-82 R2 ICS

FFC Workshops

“8 Star Memo”



COMMANDER, U.S. PACIFIC COMMAND
(USPACOM)
CAMP H.M. SMITH, HAWAII 96861-4028

February 11, 2016

The Honorable Ash Carter
Secretary of Defense
The Pentagon, Washington D.C.

Mr. Secretary,

We respectfully request your assistance in providing focus and visibility on an emerging threat that we believe will have serious consequences on our ability to execute assigned missions if not addressed – cybersecurity of DOD critical infrastructure Industrial Control Systems (ICS). We believe this issue is important enough to eventually include in your cyber scorecard. We must establish clear ownership policies at all levels of the Department, and invest in detection tools and processes to baseline normal network behavior from abnormal behavior. Once we've established this accountability, we should be able to track progress for establishing acceptable cybersecurity for our infrastructure ICS.

The Department of Homeland Security reported a seven-fold increase in cyber incidents between 2010 and 2015 on critical infrastructure (e.g., Platform Information Technology (PIT) systems, ICS, and Supervisory Control and Data Acquisition (SCADA) systems) that control the flow of electricity, water, fuel, etc. Many nefarious cyber payloads (e.g., Shamoon, Shodan, Havex and BlackEnergy) and emerging ones have the potential to debilitate our installations' mission critical infrastructure.

As Geographic Combatant Commanders with homeland defense responsibilities and much at stake in this new cyber-connected world, we request your support.

Sincerely and Very Respectfully,

WILLIAM E. GORTNEY
Admiral, U.S. Navy
Commander, U.S. Northern Command

Sincerely and Very Respectfully,

Harry Harris

HARRY B. HARRIS
Admiral, U.S. Navy
Commander, U.S. Pacific Command

- Establish Clear Ownership
- Include in Scorecard
- Invest in Detection Tools
- 7x cyber incidents

NDAA 2017

DoD facilities transitioning to smart buildings; increased connectivity has increased threat and vulnerability to cyber-attacks, particularly in ways existing DoD regulations were not designed to consider. Therefore, SECDEF deliver a report:

(1) Structural risks inherent in control systems and networks, and potential consequences associated with compromise through a cyber event;

(2) Assesses the current vulnerabilities to cyber attack initiated through Control Systems (CS) at DoD installations worldwide, determining risk mitigation actions for current and future implementation;

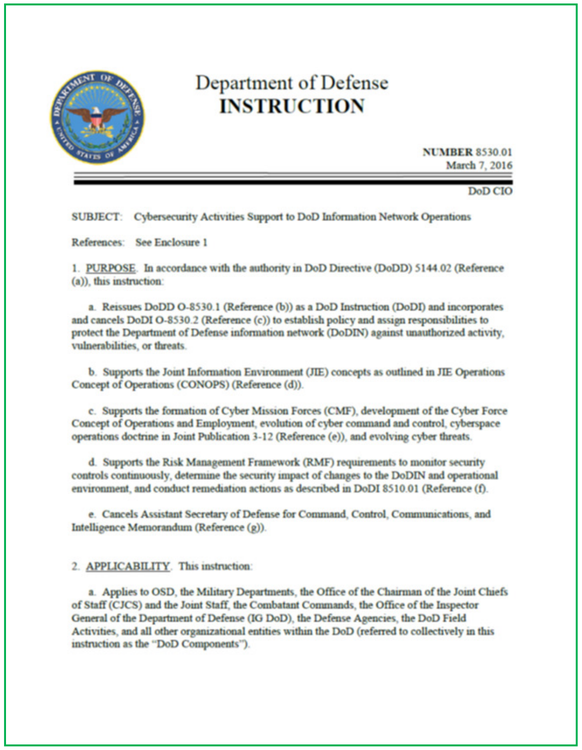
(3) Propose a common, DoD-wide implementation plan to upgrade & improve security of CS and networks to mitigate identified risks;

(4) Assesses DoD construction directives, regulations, and instructions; require the consideration of cybersecurity vulnerabilities and cyber risk in preconstruction design processes and requirements development processes for military construction projects; and

(5) Assess capabilities of Army Corps of Engineers, Naval Facilities Engineering Command, Air Force Civil Engineer Center, and other construction agents, as well as participating stakeholders, to identify and mitigate full-spectrum cyber-enabled risk to new facilities and major renovations.

CS include, but are not limited to, Supervisory Control and Data Acquisition Systems, Building Automation Systems Utility Monitoring and Energy Management and Control Systems. Such report shall include an estimated budget for the implementation plan, and delivered no later than 180 days after the date of the enactment of this Act.

DoDI 8530



Department of Defense
INSTRUCTION

NUMBER 8530.01
March 7, 2016

DoD CIO

SUBJECT: Cybersecurity Activities Support to DoD Information Network Operations

References: See Enclosure 1

1. PURPOSE. In accordance with the authority in DoD Directive (DoDD) 5144.02 (Reference (a)), this instruction:

a. Reissues DoDD O-8530.1 (Reference (b)) as a DoD Instruction (DoDI) and incorporates and cancels DoDI O-8530.2 (Reference (c)) to establish policy and assign responsibilities to protect the Department of Defense information network (DoDIN) against unauthorized activity, vulnerabilities, or threats.

b. Supports the Joint Information Environment (JIE) concepts as outlined in JIE Operations Concept of Operations (CONOPS) (Reference (d)).

c. Supports the formation of Cyber Mission Forces (CMF), development of the Cyber Force Concept of Operations and Employment, evolution of cyber command and control, cyberspace operations doctrine in Joint Publication 3-12 (Reference (e)), and evolving cyber threats.

d. Supports the Risk Management Framework (RMF) requirements to monitor security controls continuously, determine the security impact of changes to the DoDIN and operational environment, and conduct remediation actions as described in DoDI 8510.01 (Reference (f).

e. Cancels Assistant Secretary of Defense for Command, Control, Communications, and Intelligence Memorandum (Reference (g)).

2. APPLICABILITY. This instruction:

a. 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 instruction as the "DoD Components").

2. APPLICABILITY. This instruction:

b. Applies to the DoDIN. The DoDIN includes DoD information technology (IT) (e.g., DoD-owned or DoD-controlled information systems (ISs), platform information technology (PIT) systems, IT products and services) as defined in DoDI 8500.01 (Reference (h)) **and control systems and industrial control systems (ICS)** as defined in National Institute (NIST) Special Publication (SP) 800-82 (Reference (i)) that are **owned or operated by or on behalf of DoD Components**.

Continuous Monitoring and Attack Surfaces

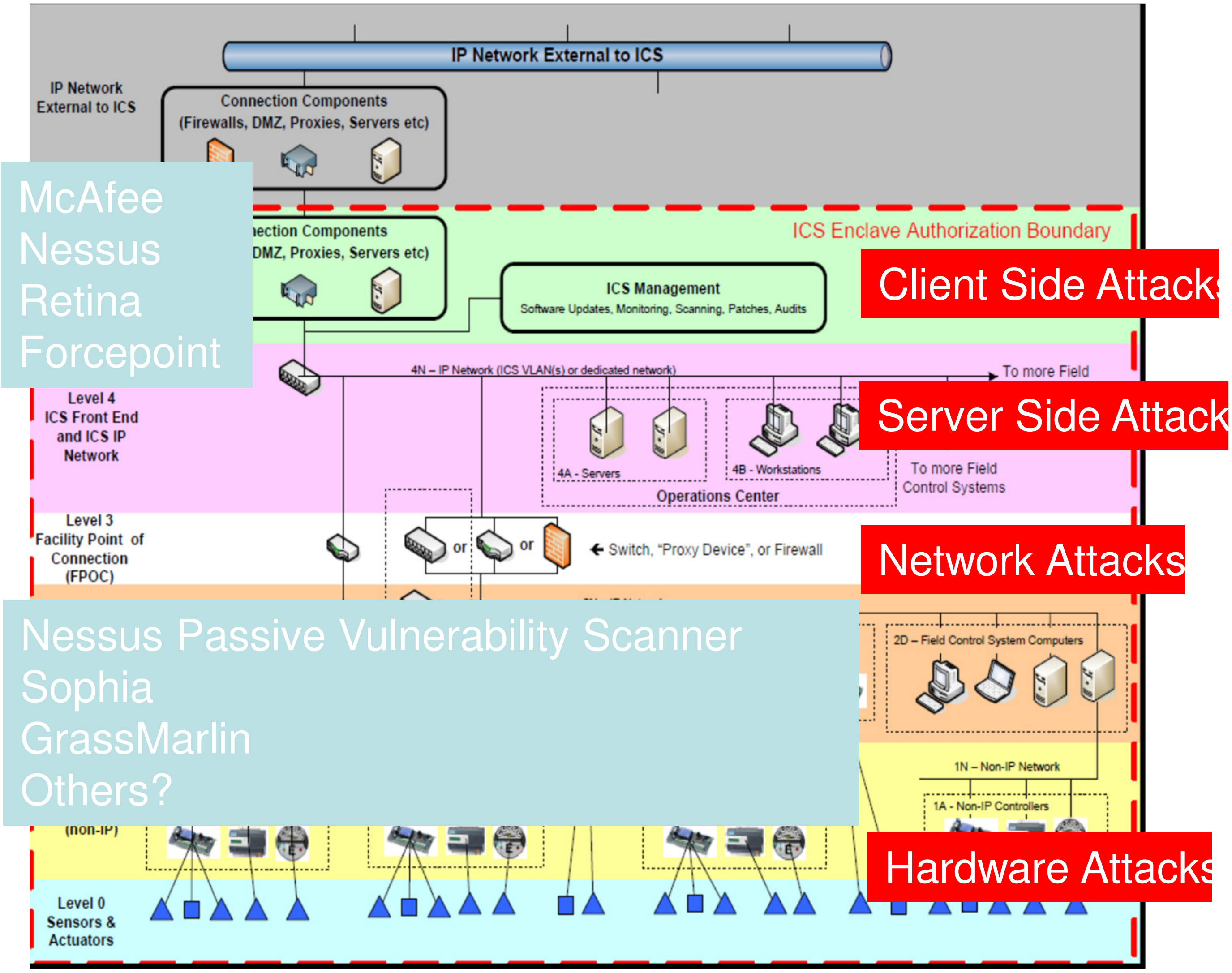
Host Based
Security Systems
Scanning (Active)

Windows, Linux
HTTP, TCP, UDP

McAfee
Nessus
Retina
Forcepoint

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

Nessus Passive Vulnerability Scanner
Sophia
GrassMarlin
Others?


IP Network External to ICS
IP Network External to ICS
Connection Components (Firewalls, DMZ, Proxies, Servers etc)
ICS Enclave Authorization Boundary
nection Components
DMZ, Proxies, Servers etc)
ICS Management
Software Updates, Monitoring, Scanning, Patches, Audits
4N – IP Network (ICS VLAN(s) or dedicated network)
To more Field
Level 4 ICS Front End and ICS IP Network
4A - Servers
4B - Workstations
Operations Center
To more Field Control Systems
Level 3 Facility Point of Connection (FPOC)
or
or
Switch, "Proxy Device", or Firewall
2D – Field Control System Computers
1N – Non-IP Network
1A - Non-IP Controllers
(non-IP)
Level 0 Sensors & Actuators

Client Side Attacks

Server Side Attack

Network Attacks

Hardware Attacks

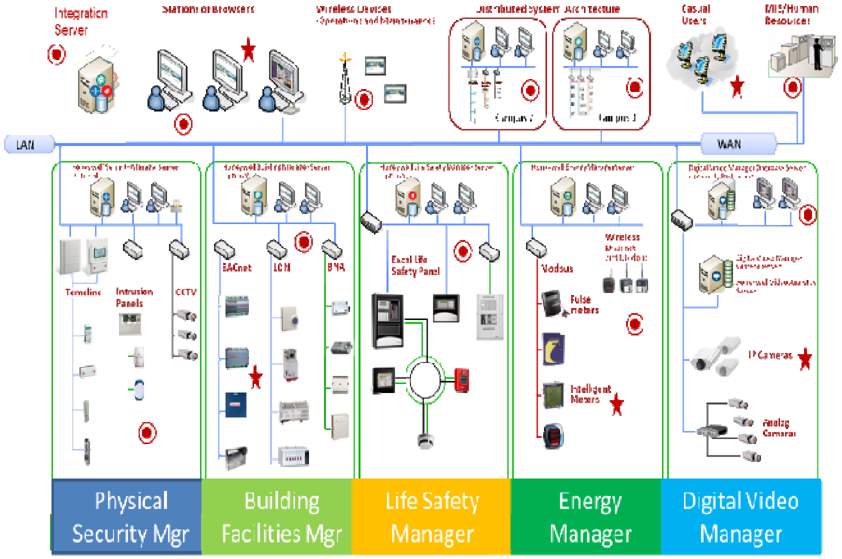
What’s Next?

- DoD CIO Control Systems Scorecard Fall 2016
- Platform Resilience Mission Assurance effort starts Spring 2016
- JHUI-APL Cyber Threats, Gaps, Workforce Reports Fall 2016
- Cyber Ranges Control Systems Competition 2017
- Acquisition and contract language to require contractors and vendors IT Business Systems to meet DoD standards (NIST SP 800-161) per DFAR 2015 – Compliance Date: Dec 2017

DoD
Real Property
Portfolio

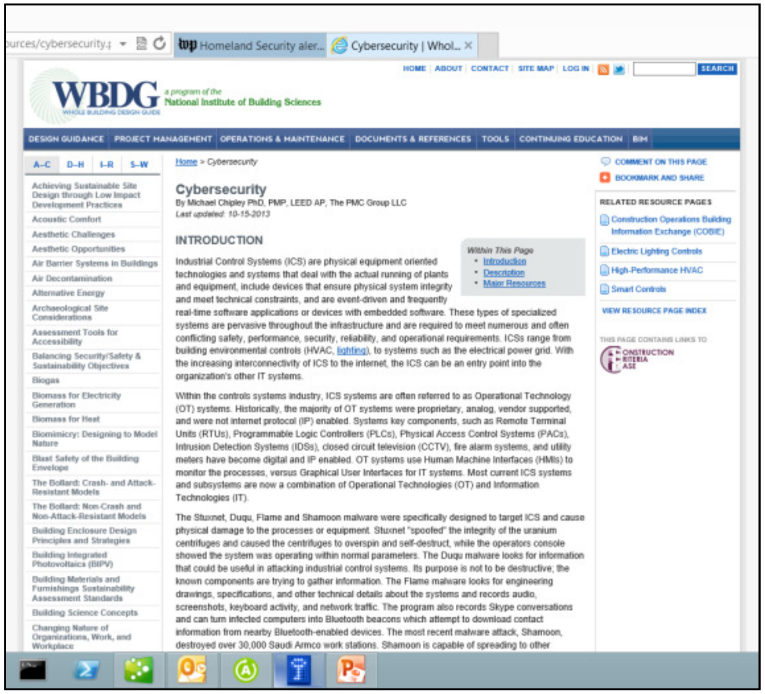
- 48 countries
- 523 installations
- 4,855 Sites
- 562,600 buildings and structures
- 24.7 M acres
- $847 B value

What’s in Your Building?



★ Possible entry point of attack ◉ Potential compromise

TTP Website Access WBDG and RMF KS


urces/cybersecurity.p
Homeland Security aler...
Cybersecurity | Whol...
HOME | ABOUT | CONTACT | SITE MAP | LOG IN
SEARCH
WBDG
WHOLE BUILDING DESIGN GUIDE
a program of the
National Institute of Building Sciences
DESIGN GUIDANCE
PROJECT MANAGEMENT
OPERATIONS & MAINTENANCE
DOCUMENTS & REFERENCES
TOOLS
CONTINUING EDUCATION
BIM
A–C
D–H
I–R
S–W
Achieving Sustainable Site Design through Low Impact Development Practices
Acoustic Comfort
Aesthetic Challenges
Aesthetic Opportunities
Air Barrier Systems in Buildings
Air Decontamination
Alternative Energy
Archaeological Site Considerations
Assessment Tools for Accessibility
Balancing Security/Safety & Sustainability Objectives
Biogas
Biomass for Electricity Generation
Biomass for Heat
Biomimicry: Designing to Model Nature
Blast Safety of the Building Envelope
The Bollard: Crash- and Attack-Resistant Models
The Bollard: Non-Crash and Non-Attack-Resistant Models
Building Enclosure Design Principles and Strategies
Building Integrated Photovoltaics (BIPV)
Building Materials and Furnishings Sustainability Assessment Standards
Building Science Concepts
Changing Nature of Organizations, Work, and Workplace
COMMENT ON THIS PAGE
BOOKMARK AND SHARE
RELATED RESOURCE PAGES
Construction Operations Building Information Exchange (COBIE)
Electric Lighting Controls
High-Performance HVAC
Smart Controls
VIEW RESOURCE PAGE INDEX
THIS PAGE CONTAINS LINKS TO
CONSTRUCTION CRITERIA BASE

Home > Cybersecurity

Cybersecurity

By Michael Chipley PhD, PMP, LEED AP, The PMC Group LLC

Last updated: 10-15-2013

INTRODUCTION

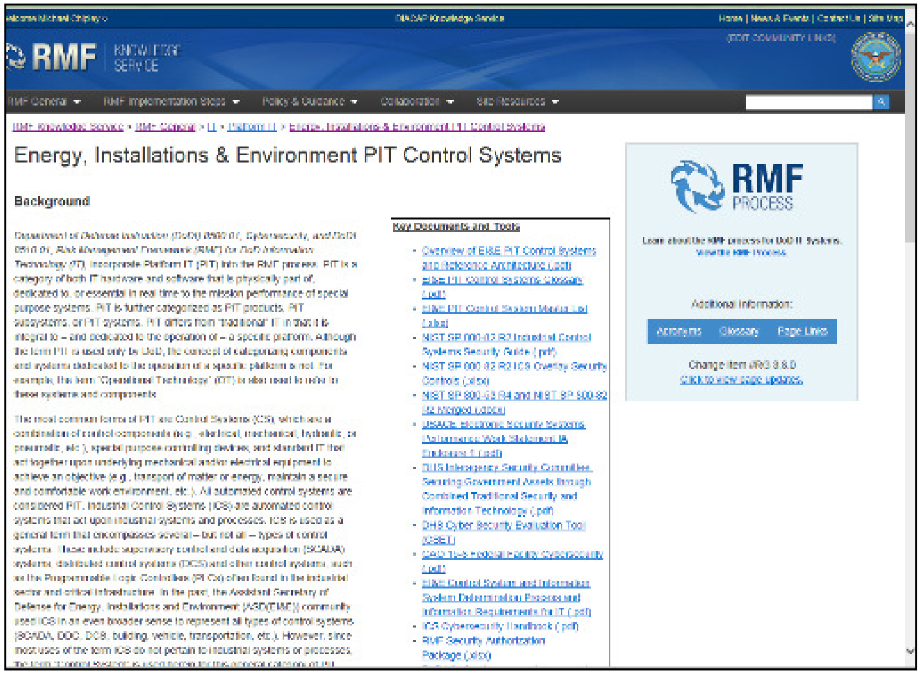
Within This Page

- Introduction
- Description
- Major Resources

Industrial Control Systems (ICS) are physical equipment oriented technologies and systems that deal with the actual running of plants and equipment, include devices that ensure physical system integrity and meet technical constraints, and are event-driven and frequently real-time software applications or devices with embedded software. These types of specialized systems are pervasive throughout the infrastructure and are required to meet numerous and often conflicting safety, performance, security, reliability, and operational requirements. ICSs range from building environmental controls (HVAC, lighting), to systems such as the electrical power grid. With the increasing interconnectivity of ICS to the internet, the ICS can be an entry point into the organization's other IT systems.

Within the controls systems industry, ICS systems are often referred to as Operational Technology (OT) systems. Historically, the majority of OT systems were proprietary, analog, vendor supported, and were not internet protocol (IP) enabled. Systems key components, such as Remote Terminal Units (RTUs), Programmable Logic Controllers (PLCs), Physical Access Control Systems (PACs), Intrusion Detection Systems (IDSs), closed circuit television (CCTV), fire alarm systems, and utility meters have become digital and IP enabled. OT systems use Human Machine Interfaces (HMIs) to monitor the processes, versus Graphical User Interfaces for IT systems. Most current ICS systems and subsystems are now a combination of Operational Technologies (OT) and Information Technologies (IT).

The Stuxnet, Duqu, Flame and Shamoon malware were specifically designed to target ICS and cause physical damage to the processes or equipment. Stuxnet "spoofed" the integrity of the uranium centrifuges and caused the centrifuges to overspin and self-destruct, while the operators console showed the system was operating within normal parameters. The Duqu malware looks for information that could be useful in attacking industrial control systems. Its purpose is not to be destructive; the known components are trying to gather information. The Flame malware looks for engineering drawings, specifications, and other technical details about the systems and records audio, screenshots, keyboard activity, and network traffic. The program also records Skype conversations and can turn infected computers into Bluetooth beacons which attempt to download contact information from nearby Bluetooth-enabled devices. The most recent malware attack, Shamoon, destroyed over 30,000 Saudi Armco work stations. Shamoon is capable of spreading to other



RMF Knowledge Service > RMF General > IT > Platform IT > Energy, Installations & Environment PIT Control Systems

Energy, Installations & Environment PIT Control Systems

Background

Department of Defense Instruction (DoDI) 8500.01, *Cybersecurity*, and DoDI 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT)*, incorporate Platform IT (PIT) into the RMF process. PIT is a category of both IT hardware and software that is physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems. PIT is further categorized as PIT products, PIT subsystems, or PIT systems. PIT differs from "traditional" IT in that it is integral to – and dedicated to the operation of – a specific platform. Although the term PIT is used only by DoD, the concept of categorizing components and systems dedicated to the operation of a specific platform is not. For example, the term "Operational Technology" (OT) is also used to refer to these systems and components.

The most common forms of PIT are Control Systems (CS), which are a combination of control components (e.g., electrical, mechanical, hydraulic, or pneumatic, etc.), special purpose controlling devices, and standard IT that act together upon underlying mechanical and/or electrical equipment to achieve an objective (e.g., transport of matter or energy, maintain a secure and comfortable work environment, etc.). All automated control systems are considered PIT. Industrial Control Systems (ICS) are automated control systems that act upon industrial systems and processes. ICS is used as a general term that encompasses several – but not all – types of control systems. These include supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS) and other control systems, such as the Programmable Logic Controllers (PLCs) often found in the industrial sector and critical infrastructure. In the past, the Assistant Secretary of Defense for Energy, Installations and Environment (ASD(EI&E)) community used ICS in an even broader sense to represent all types of control systems (SCADA, DDC, DCS, building, vehicle, transportation, etc.). However, since most uses of the term ICS do not pertain to industrial systems or processes, the term "Control Systems" is used herein for the general category of PIT

Key Documents and Tools

- Overview of EI&E PIT Control Systems and Reference Architecture (.pdf)
- EI&E PIT Control Systems Glossary (.pdf)
- EI&E PIT Control System Master List (.xlsx)
- NIST SP 800-82 R2 Industrial Control Systems Security Guide (.pdf)
- NIST SP 800-82 R2 ICS Overlay Security Controls (.xlsx)
- NIST SP 800-53 R4 and NIST SP 800-82 R2 Merged (.xlsx)
- USACE Electronic Security Systems Performance Work Statement IA Enclosure 1 (.pdf)
- DHS Interagency Security Committee, Securing Government Assets through Combined Traditional Security and Information Technology (.pdf)
- DHS Cyber Security Evaluation Tool (CSET)
- GAO 15-6 Federal Facility Cybersecurity (.pdf)
- EI&E Control System and Information System Determination Process and Information Requirements for IT (.pdf)
- ICS Cybersecurity Handbook (.pdf)
- RMF Security Authorization Package (.xlsx)

1.Navigate to DoD CIO Knowledge Service (requires CAC)
https://rmfks.osd.mil/login.htm

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

TTP ‘s Apply to IT and OT

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

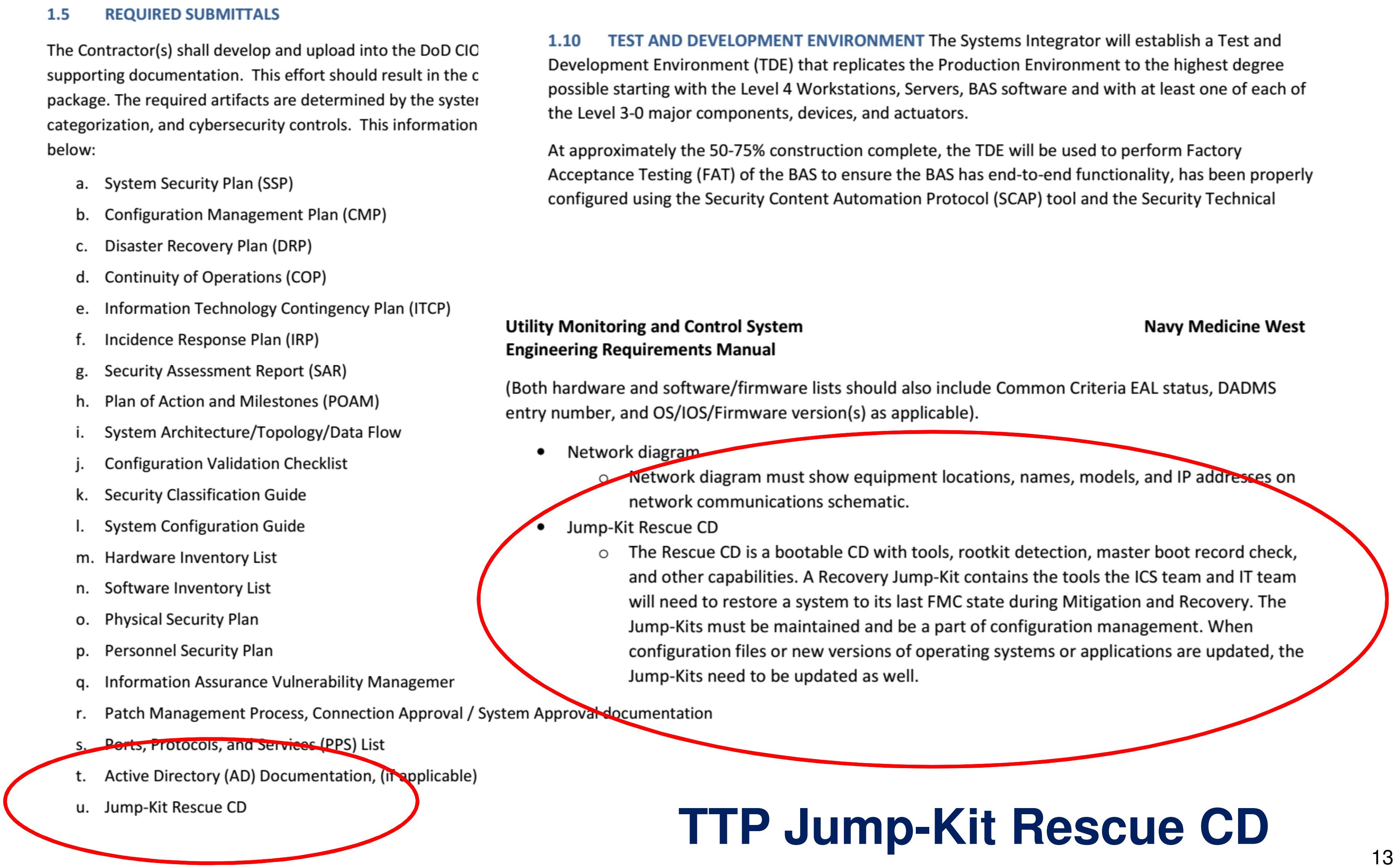
Information Technology (IT) Systems – Business and Home
Operational Technologies (OT) Systems – Any Kind (Utility, Building, Environmental, Medical, Logistics, Transportation, Weapons, etc.)

At the conclusion of the workshop, you will appreciate your IT and OT networks in a new way and have situational awareness of normal versus abnormal behavior, know what actions to take, what contract language to add to SOW’s, and how to protect sensitive information as the Internet of Things and the convergence of IT and OT continues to evolve.

For the foreseeable future, the trend to co-mingle IT and OT building control systems data on non-segmented networks is likely to be the norm; DON’T BE A TREND FOLLOWER, DON’T DO IT!

- ***Segment and VLAN IT and OT networks***
- ***Separate the OS and OT data (C: OS and D: OT data), enable BitLocker on OT drive***

New Draft Navy IA Guidance with the TTP’s



1.5 REQUIRED SUBMITTALS

The Contractor(s) shall develop and upload into the DoD CIO supporting documentation. This effort should result in the c package. The required artifacts are determined by the syster categorization, and cybersecurity controls. This information 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 Managemer
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

1.10 TEST AND DEVELOPMENT ENVIRONMENT 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, BAS 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 BAS to ensure the BAS has end-to-end functionality, has been properly configured using the Security Content Automation Protocol (SCAP) tool and the Security Technical

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

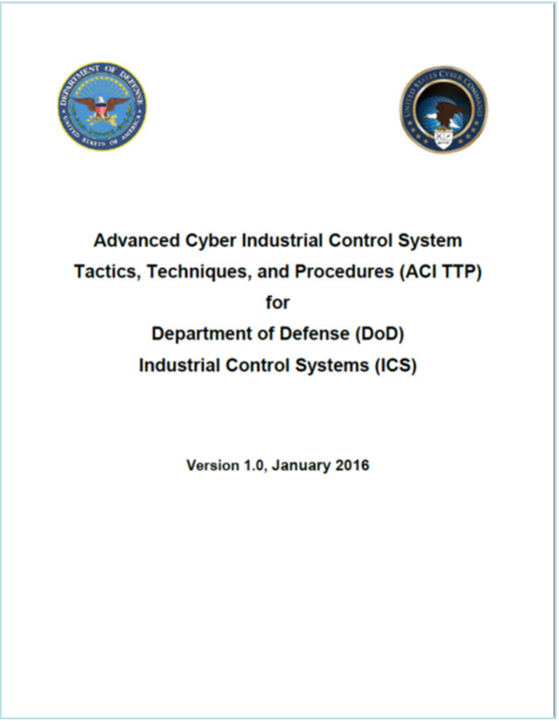
(Both hardware and software/firmware lists should also include Common Criteria EAL status, DADMS entry number, and OS/IOS/Firmware version(s) as applicable).

- 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

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.**



Advanced Cyber Industrial Control System
Tactics, Techniques, and Procedures (ACI TTP)
for
Department of Defense (DoD)
Industrial Control Systems (ICS)

Version 1.0, January 2016

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)

ACT TTP Concepts

ACI TTP Concepts. The concepts provide background information to assist in explaining the scope, prerequisites, applicability, and limitations of the components of this TTP. The concept chapters should be read prior to responding to indication of malicious cyber activity.

In the 1990s, in order to leverage newly identified efficiencies in ICS, formerly physically isolated ICS networks were adapted to interface with the Internet. In the early 2000s, active cyber threats were still in their infancy. However, today the cyber threat to ICS has grown from an obscure annoyance to one of the most significant threats to national security (Rogers, 2015).

The threat, coupled with the inherent lack of cyber security and a long-life span for ICS equipment, has created ideal conditions for a cyber attack causing physical and tangible repercussions. This has led to a need for tactics, techniques, and procedures (TTP) relative to the operations of traditional ICS equipment as well as information technology (IT) components.

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

Baselining and Routine Monitoring of the Network.

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.**

Fully-Mission Capable (FMC Baseline) and Jump-Kit Rescue CD are critical to implement Defend, Mitigate and Recover portions of the TTP

Reference Materials

Reference Materials.

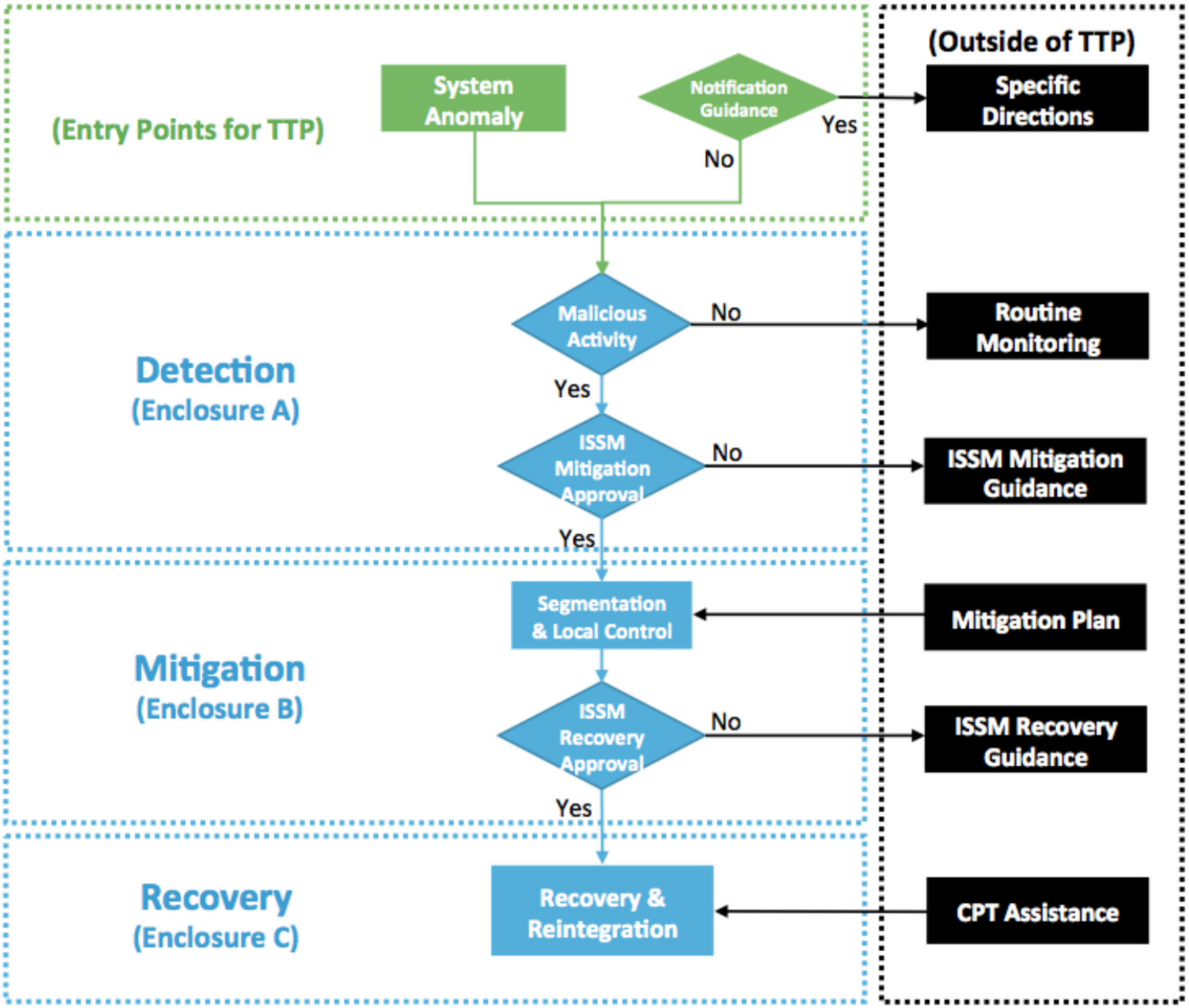
To further enhance the ACI TTP as a tool, **operators are encouraged to refer to additional resources provided by the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) and the National Institute of Standards and Technology (NIST) Special Publication (SP) 800 Computer Security series** (see Appendix D: References).

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, Mitigation, Recovery Overview



Detection

a. Detection.

When a notification is received or an anomalous symptom is observed, the operator should locate the symptom on the *Event Diagnostics Table* (enclosure A.1 , table A.1.1). After locating and investigating the event diagnostics (which includes eliminating any non-cyber causes for the anomaly), the operator is directed to the *Integrity Checks Table* (enclosure A, section A.3, table A.3.1). **These checks provide actions which assists the operator in determining whether a cyber event is in progress or not.** The operator returns to the diagnostic procedure and then decides either to continue with another integrity check or exit the procedure by moving to the Mitigation section or returning to the Routine Monitoring section (enclosure D). In the case of malicious cyber activity, specific reporting procedures are provided. The operator is then directed to notify the ISSM and request permission to move to the Mitigation section.

Mitigation

b. Mitigation.

If the ISSM confirms permission to move to the Mitigation section, **the operator's first priority is to isolate any compromised assets, and protect the commander's mission priority through segmentation.** This segmentation is based on a predetermined segmentation strategy. After this step is complete, the operator next ensures that local control has been achieved. **After the system is stabilized, the operator can make a request to the ISSM to proceed to the Recovery section.**

For commercial office and non-government BCS, the owner or property manager determines the priorities; in most cases tenant service level agreements have pre-defined requirements.

It may not be possible to isolate all segments and the decision to continue using the compromised BCS in a degraded mode may be the best option.

If the IT and OT data is on the same segment (not on separate VLAN)'s, it should be assumed that ALL BCS and owner and tenant IT systems are potentially exploited.

Recovery

c. Recovery.

Recovery actions follow Mitigation actions. While the TTP addresses specific Recovery actions, **operators may need to execute investigations, incident response plans, and various other overarching command guidelines prior to executing any Recovery actions.** Operators should ensure familiarity with these policies and guidelines.

Maintaining Operational Resilience

Maintaining Operational Resilience

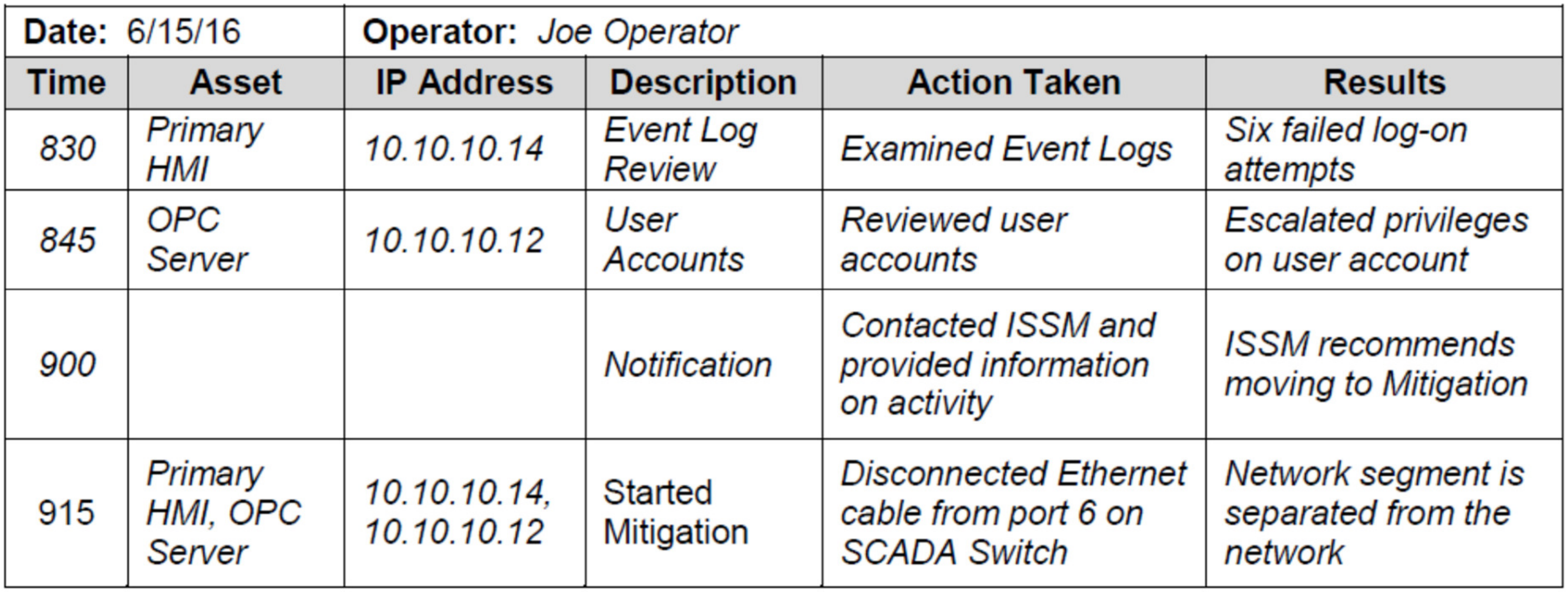
As cyber attacks have become focused and relevant in the world of cyber warfare, the DoD has moved from a position of “system hardening” to a posture of maintaining operational resilience. With the release of Department of Defense Instruction (DoDI) 8500.01, *Cybersecurity*, in March of 2014, the DoD addresses the fact that cyber attacks are inevitable, and adversaries will succeed to some degree. Therefore, it is incumbent upon all operational areas of the DoD to be prepared to meet these three conditions: ensure systems are trustworthy, ensure the mission of the organization is prepared to operate with degraded capabilities, and ensure systems have the means to prevail in the face of adverse events.

The ACI TTP provides ICS operators with a means to use both best practices and procedures in the defense of the ICS, to degrade the ICS, if necessary, and to maintain system operations during an active cyber attack.

Operational Security Log

Operational Security Log

There are instructions throughout the ACI TTP threat-response procedures sections (enclosures A through C) to record information in a Security Log. **An operational Security Log is a written organizational record of events such that a reconstruction of events could occur to illustrate, over time, the adversarial cyber events that occurred on an ICS/IT network as well as the organizational actions to Detect and/or counteract them.** A log should be designed to reflect and accommodate your environment and o



Date: 6/15/16		**Operator:** *Joe Operator*			
Time	**Asset**	**IP Address**	**Description**	**Action Taken**	**Results**
830	*Primary HMI*	*10.10.10.14*	*Event Log Review*	*Examined Event Logs*	*Six failed log-on attempts*
845	*OPC Server*	*10.10.10.12*	*User Accounts*	*Reviewed user accounts*	*Escalated privileges on user account*
900			*Notification*	*Contacted ISSM and provided information on activity*	*ISSM recommends moving to Mitigation*
915	*Primary HMI, OPC Server*	*10.10.10.14, 10.10.10.12*	Started Mitigation	*Disconnected Ethernet cable from port 6 on SCADA Switch*	*Network segment is separated from the network*

Chapter 2 – Detection Concepts

Detection Introduction

a. Definition. The identification of evidence of an adversarial presence, or the determination of no adversarial presence

b. Key Components

(1) Routine Monitoring
(2) Inspection
(3) Identification of adversarial presence
(4) Documentation
(5) Notifications

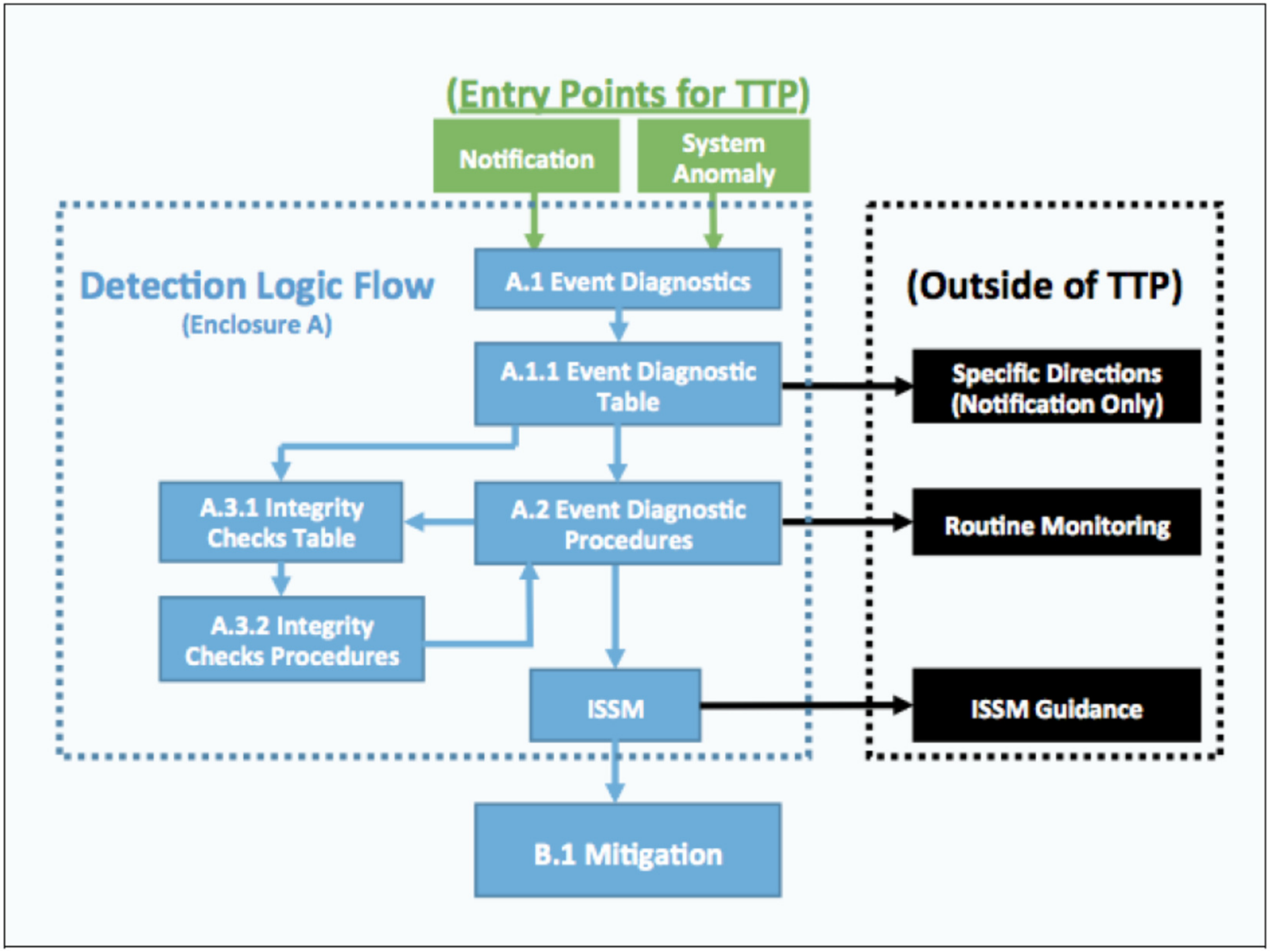
c. Prerequisites

(1) FMC baseline
(2) Routine Monitoring
(3) Security Log

Detection Process ACI TTP Entry Points

1. Anomalies found during Routine Monitoring
2. Organization directives, ICS-CERT Notices or other official notifications

Detection Entry Points



Chapter 3 – Mitigation Concepts

Mitigation Introduction

a. Definition. The actions taken that allow the CS network to continue operating after the operator has separated the affected device and/or network segment to prevent the propagation of the adversarial presence and to establish control to allow end-state processes to continue to operate at the command-directed level without interference.

b. Key Components

(1) Protect the information network
(2) Acquire and protect data for analysis
(3) Maintain operations during an active attack

c. Prerequisites

(1) Identification of evidence of an adversarial presence
(2) Appropriate notifications and reporting have been initiated
(3) Security Log

Chapter 3 – Mitigation Concepts (cont)

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

Recovery Introduction

a. Description. Restoration and reintegration of the CS to a FOC state.

b. Key Components

(1) Identify mission priorities
(2) Acquire and protect data for analysis
(3) Systematically Recover each affected device
(4) Systematically reintegrate devices, processes, and network segments
(5) Test and verify system to ensure devices are not re-infected

c. Prerequisites

(1) Network has been isolated and stabilized from the cyber-incident
(2) Appropriate notifications and reporting has occurred
(3) Response Jump-Kit
(4) Baseline documentation

Chapter 4 – Recovery Concepts (cont)

The operator **must not** proceed with Recovery Procedures without proper authorization and should consult with the ISSM prior to proceeding with those Recovery Procedures. A CPT from outside your organization may be called upon to direct the Recovery process. **The main focus of the CPT is to preserve forensic evidence for analysis of the cyber incident and to provide technical assistance as required.** If directed, the operator may proceed with Recovery Procedures without the assistance of a CPT. Every effort should be made to preserve evidence of the cyber incident for forensic analysis whenever feasible.

Forensic evidence collection for BCS at this time is very difficult and time consuming; very few building controllers have logs, are not authenticated, and are on unencrypted networks.

Chapter 4 – Recovery Concepts (cont)

Recovery Process

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.

Chapter 4 – Recovery Concepts (cont)

c. The **preferred method of Recovery is the removal and replacement of affected devices with off-the-shelf replacements.** This method ensures that recovered devices are uncontaminated when reintegrated into the network and will aid in preservation of forensic evidence of the cyber attack for analysis. If replacement devices are not available, the second best option is to reimage affected devices with known good firmware and/or software. **Whenever possible in this scenario, efforts should be made to save a copy of the infected firmware/software for forensic analysis. Vendor assistance may be required in order to perform these tasks.**

For most BCS, it will not be possible to replace the building controllers; a small building could have 1000 or more, a medium building 10,000 and a large building over 100,000; with multiple vendors and on equipment located throughout the building.

Chapter 4 – Recovery Concepts (cont)

d. Additional key points to effective Recovery include technical issues, mission priorities, and cyber issues:

(1) Technical Issues. **Recovery requires the ability to reintegrate affected devices into operation after they have been replaced or verified to be clean of any remnants from a cyber incident.** This TTP cannot provide specific detailed instructions on how to reintegrate each device for the wide variety of networks known to exist. **The Recovery team will be required to determine the sequence of device reintegration in order to ensure minimal effect on the operation of any critical assets in the network, and to avoid recontamination of recently cleaned devices.**

(2) Mission Priorities*.* **The sequence of Recovery and reintegration of recovered devices will depend on the mission-critical need for systems affected based upon the requirements set forth by the organization.** Be sure to consult with your ISSM and/or chain of command to ensure you are prioritizing the sequence of the Recovery process as required by your organization.

E.2. FMC Baseline Overview

E.2. FMC Baseline Overview

a. **Before the ACI TTP can be executed, operators should have several system characteristics documented. This documentation forms the system's current FMC baseline.** Documenting the FMC baseline does not imply the system may not already have an adversary present. In fact, many systems might have an adversary present. If an adversary is present, and that adversary is lying in wait, if the adversary moves laterally or attempts to communicate or otherwise initiate an exploit (and eventually the adversary will), the ACI TTP is designed to Detect that type of movement by comparing system characteristics to its baseline.

b. This section provides specific details for developing the FMC baseline of an ICS. **The FMC Baseline establishes normal ICS behavior.** During Routine Monitoring and the Detection Phase of the ACI TTP, normal behaviors are compared to observed behaviors. If observed behaviors deviate from normal behaviors, these are either by design (approved and intentional) or anomalous (unapproved, unintentional, not communicated, or nefarious).

F.1. Jump-Kit Introduction

F.1. Jump-Kit Introduction

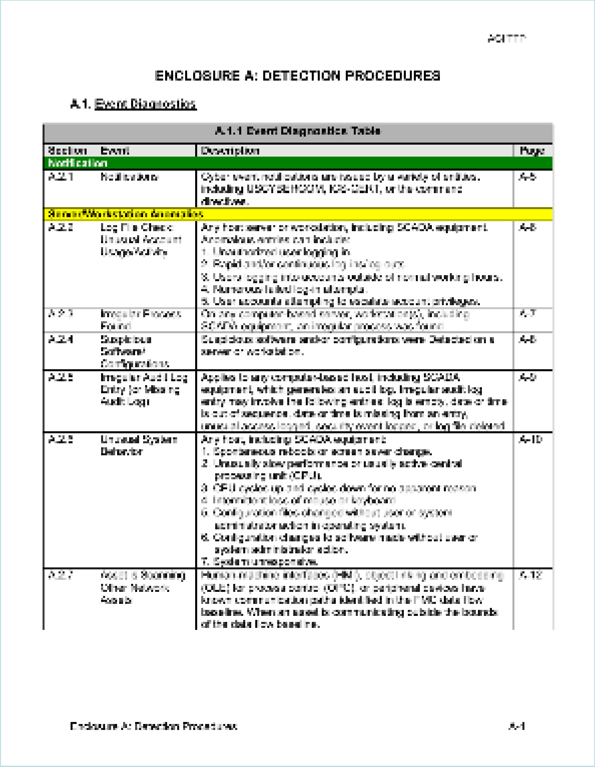
a. Description. A Recovery Jump-Kit contains the tools the ICS team and IT team will need to restore a system to its last FMC state during Mitigation and Recovery. Knowing what the Recovery point should be is the key to ensuring all known remnants of an attack have been removed from all components of the ICS. This means all hardware and software are configured in accordance with operational requirements, and checksums and hashes are in conformance with vendor specifications.

b. Key Components

(1) Routine Monitoring
(2) Inspection
(3) Identification of adversarial presence
(4) Documentation
(5) Notifications

c. Prerequisites. FMC baseline

ENCLOSURE A: DETECTION PROCEDURES



ACI TTP

ENCLOSURE A: DETECTION PROCEDURES

A.1. Event Diagnostics

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 in/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

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

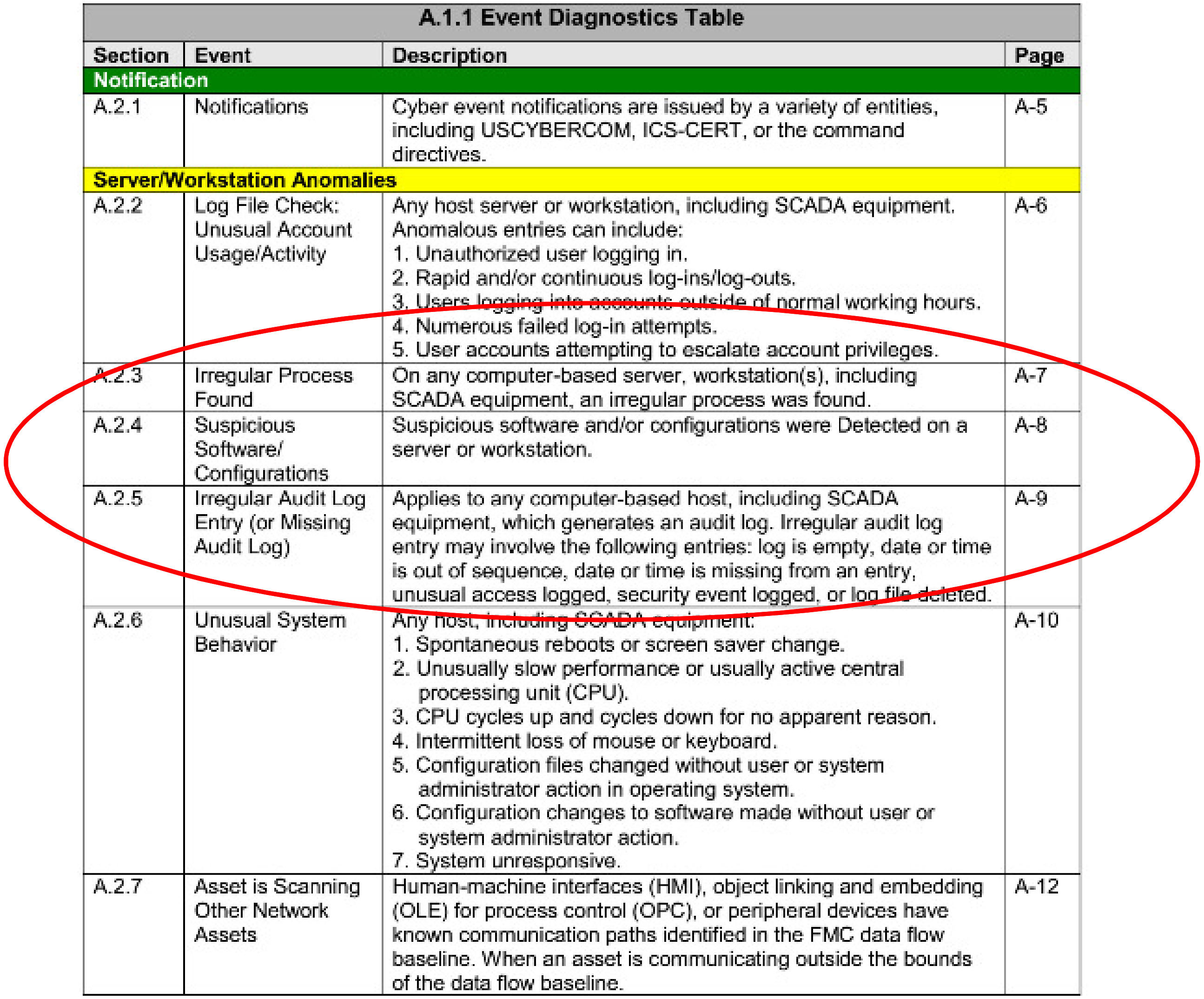
A.2.5 Server/Workstation: Irregular Audit Log Entry (Or Missing Audit Log)

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

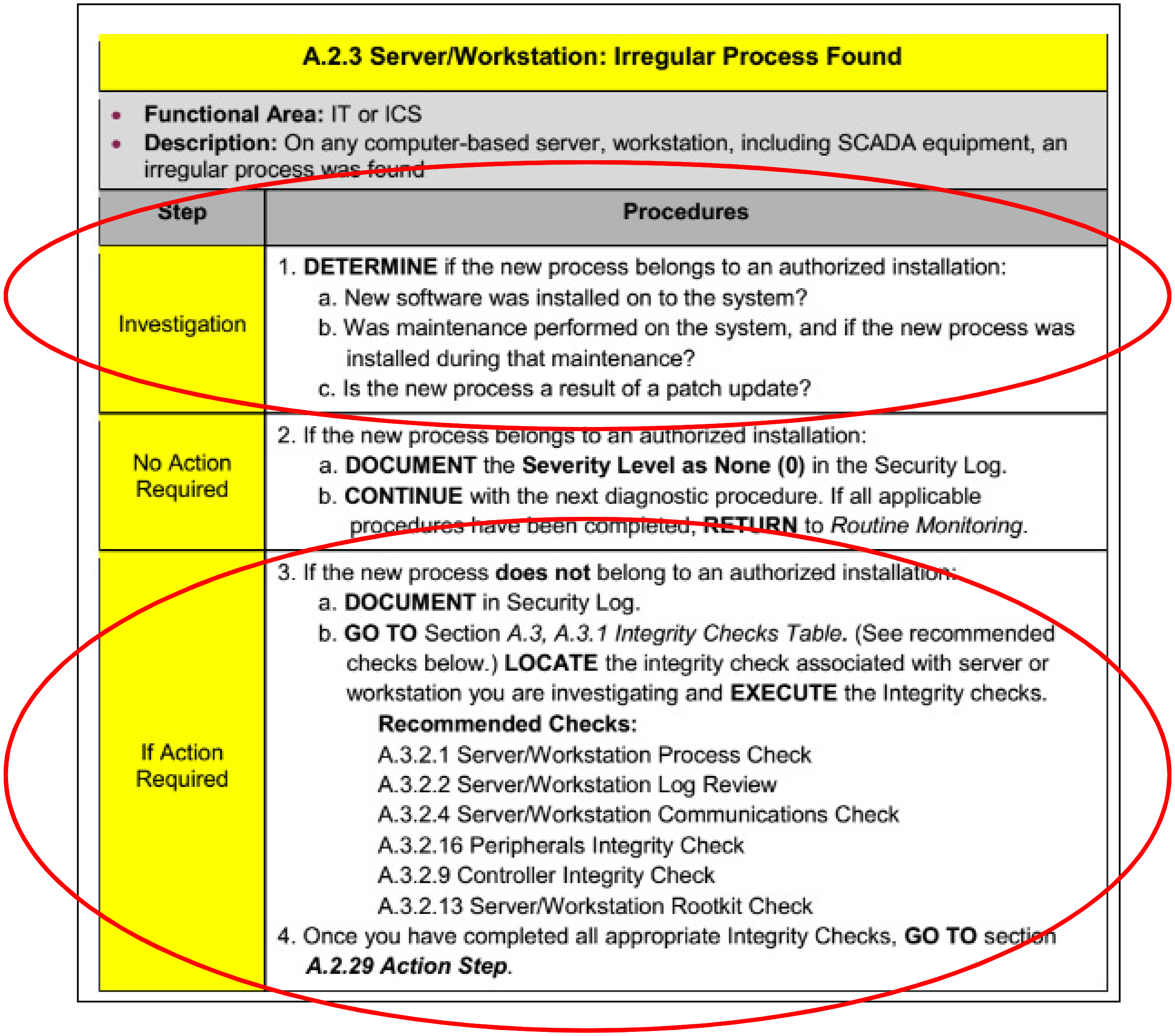
DETECTION PROCEDURES SERVER EXAMPLE 1



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: 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 1

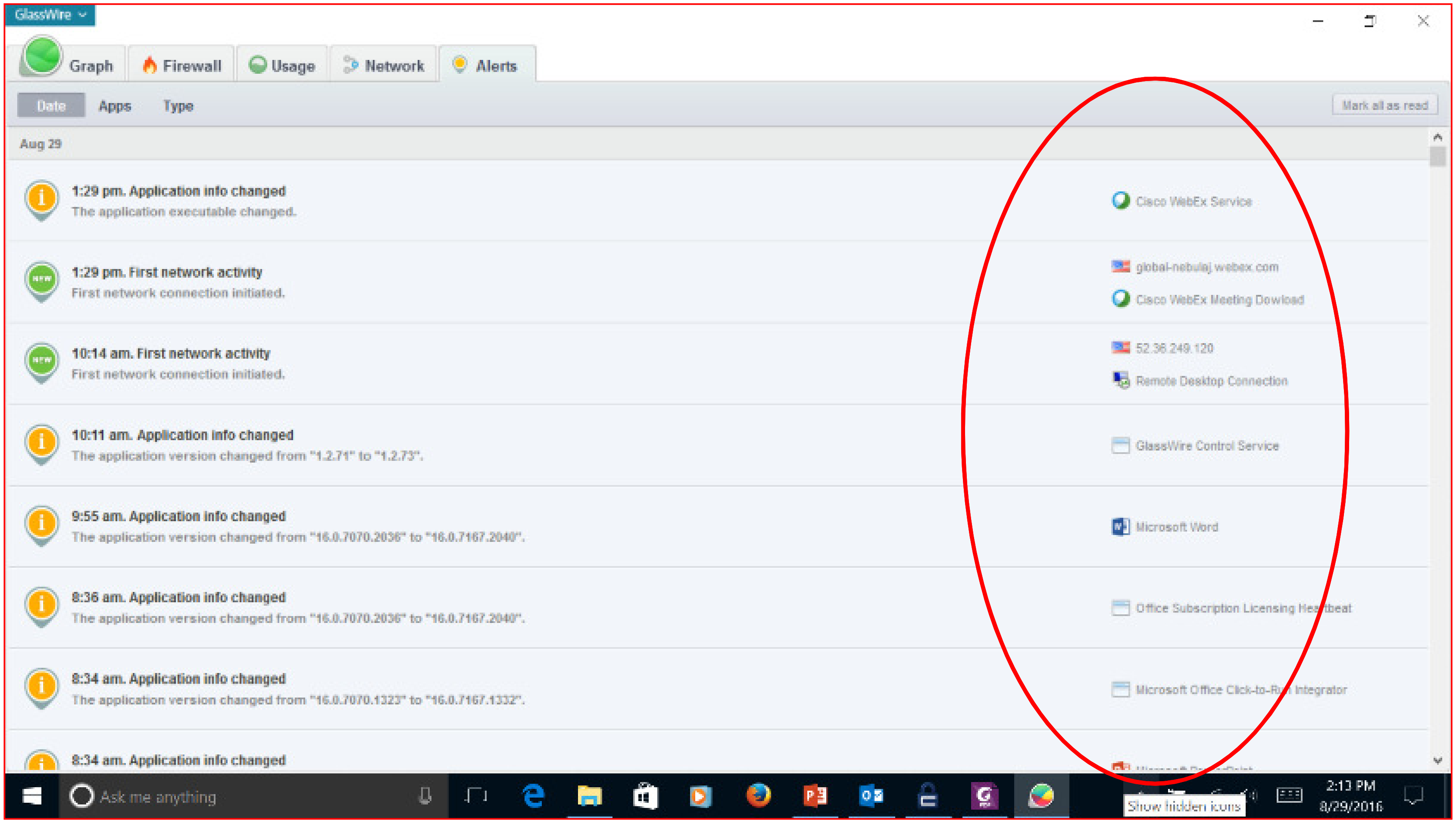


A.2.3 Server/Workstation: Irregular Process Found

- **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 1



Aug 29

1:29 pm. Application info changed
The application executable changed.
Cisco WebEx Service

1:29 pm. First network activity
First network connection initiated.
global-nebulaj.webex.com
Cisco WebEx Meeting Dowload

10:14 am. First network activity
First network connection initiated.
52.36.249.120
Remote Desktop Connection

10:11 am. Application info changed
The application version changed from "1.2.71" to "1.2.73".
GlassWire Control Service

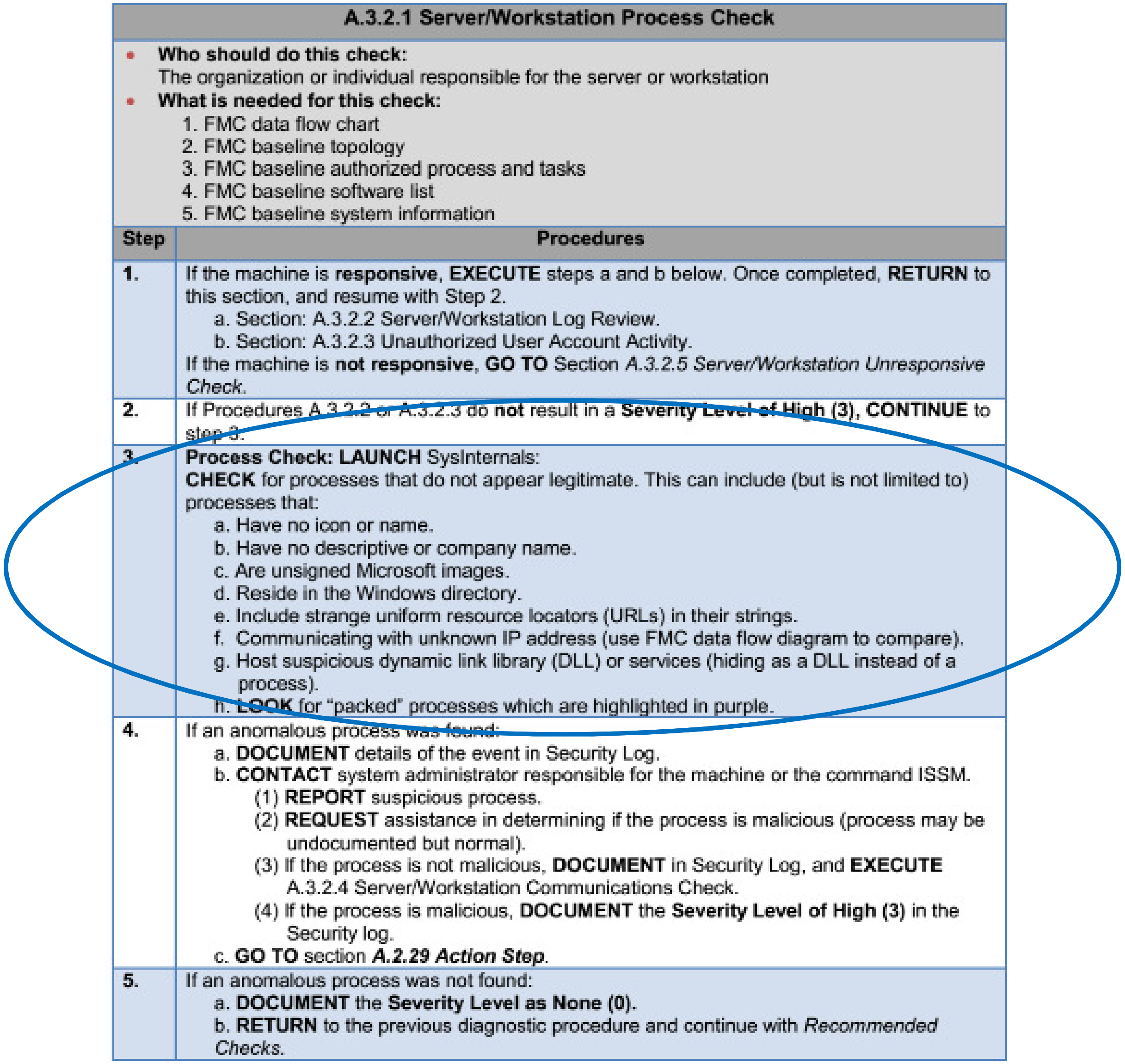
9:55 am. Application info changed
The application version changed from "16.0.7070.2036" to "16.0.7167.2040".
Microsoft Word

8:36 am. Application info changed
The application version changed from "16.0.7070.2036" to "16.0.7167.2040".
Office Subscription Licensing Heartbeat

8:34 am. Application info changed
The application version changed from "16.0.7070.1323" to "16.0.7167.1332".
Microsoft Office Click-to-Run Integrator

8:34 am. Application info changed
Microsoft PowerPoint

DETECTION PROCEDURES SERVER EXAMPLE 1

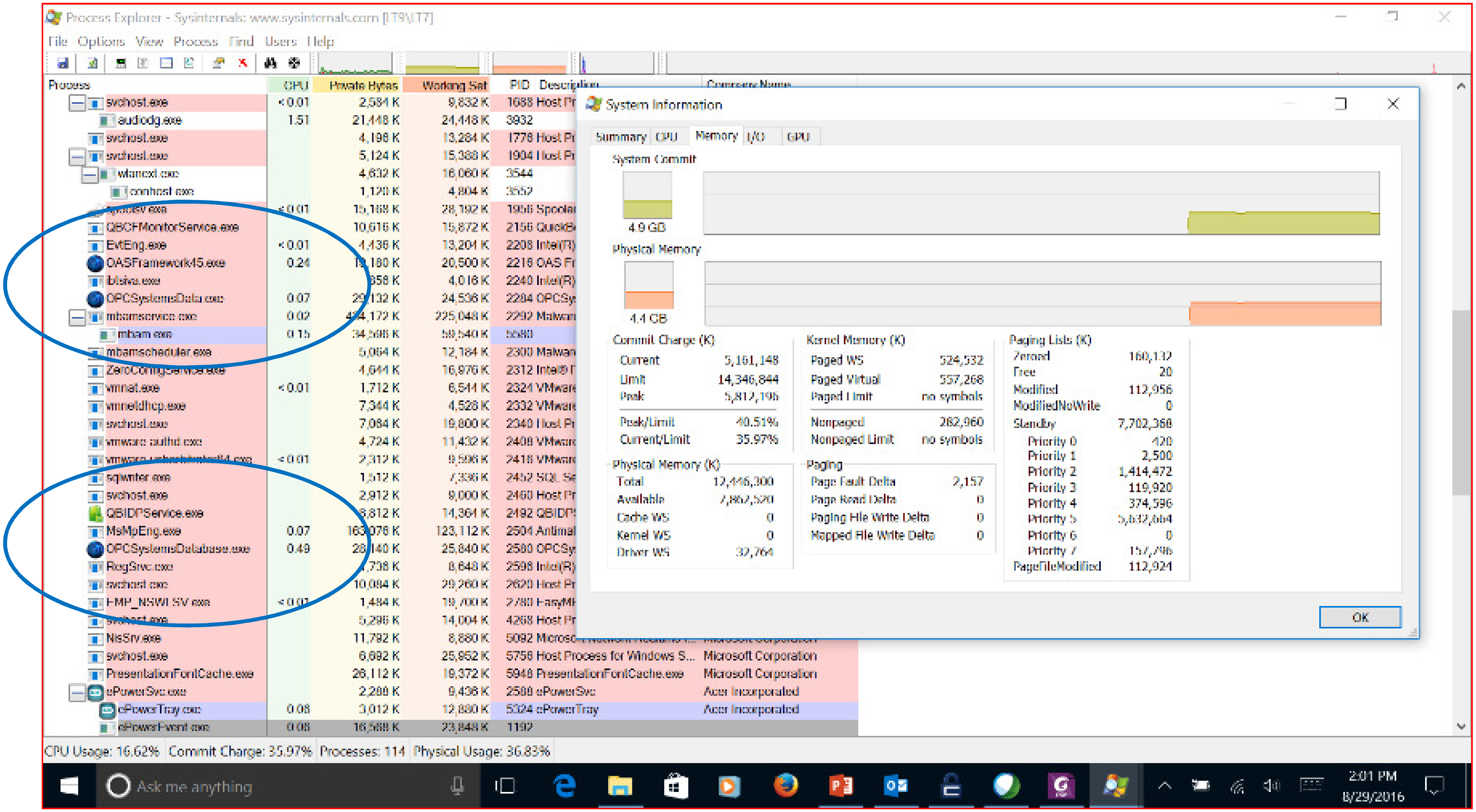


A.3.2.1 Server/Workstation Process Check

- **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 1



Process Explorer - Sysinternals: www.sysinternals.com [LT9\LT7]

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
svchost.exe	< 0.01	2,584 K	9,832 K	1688	Host Pr	
audiodg.exe	1.51	21,448 K	24,448 K	3932		
svchost.exe		4,196 K	13,284 K	1778	Host Pr	
svchost.exe		5,124 K	15,388 K	1904	Host Pr	
wlanext.exe		4,632 K	16,060 K	3544		
conhost.exe		1,120 K	4,804 K	3552		
spoolsv.exe	< 0.01	15,168 K	28,192 K	1956	Spooler	
QBCFMonitorService.exe		10,616 K	15,872 K	2156	QuickB	
EvtEng.exe	< 0.01	4,436 K	13,204 K	2208	Intel(R)	
OASFramework45.exe	0.24	19,180 K	20,500 K	2216	OAS Fr	
ibtsiva.exe		1,858 K	4,016 K	2240	Intel(R)	
OPCSystemsData.exe	0.07	29,132 K	24,536 K	2264	OPCSy	
mbamservice.exe	0.02	434,172 K	225,048 K	2292	Malwar	
mbam.exe	0.15	34,596 K	59,540 K	5580		
mbamscheduler.exe		5,064 K	12,184 K	2300	Malwar	
ZeroConfigService.exe		4,644 K	16,976 K	2312	Intel® I	
vmnat.exe	< 0.01	1,712 K	6,544 K	2324	VMware	
vmnetdhcp.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	
vmware-usbarbitrator64.exe	< 0.01	2,312 K	9,596 K	2416	VMware	
sqlwriter.exe		1,512 K	7,336 K	2452	SQL Se	
svchost.exe		2,912 K	9,000 K	2460	Host Pr	
QBIDPService.exe		3,812 K	14,364 K	2492	QBIDP	
MsMpEng.exe	0.07	163,076 K	123,112 K	2504	Antimal	
OPCSystemsDatabase.exe	0.49	28,140 K	25,840 K	2580	OPCSy	
RegSrvc.exe		1,738 K	8,648 K	2598	Intel(R)	
svchost.exe		10,084 K	29,260 K	2620	Host Pr	
EMP_NSWLSV.exe	< 0.01	1,484 K	19,700 K	2780	EasyMi	
svchost.exe		5,296 K	14,004 K	4268	Host Pr	
NisSrv.exe		11,792 K	8,880 K	5092	Microso	
svchost.exe		6,692 K	25,952 K	5756	Host Process for Windows S...	Microsoft Corporation
PresentationFontCache.exe		28,112 K	19,372 K	5948	PresentationFontCache.exe	Microsoft Corporation
ePowerSvc.exe		2,288 K	9,436 K	2588	ePowerSvc	Acer Incorporated
ePowerTray.exe	0.08	3,012 K	12,880 K	5324	ePowerTray	Acer Incorporated
ePowerEvent.exe	0.08	16,568 K	23,848 K	1192		

CPU Usage: 16.62% Commit Charge: 35.97% Processes: 114 Physical Usage: 36.83%

System Information

System Commit

4.9 GB

Physical Memory

4.4 GB

Commit Charge (K)	
Current	5,161,148
Limit	14,346,844
Peak	5,812,196
Peak/Limit	40.51%
Current/Limit	35.97%

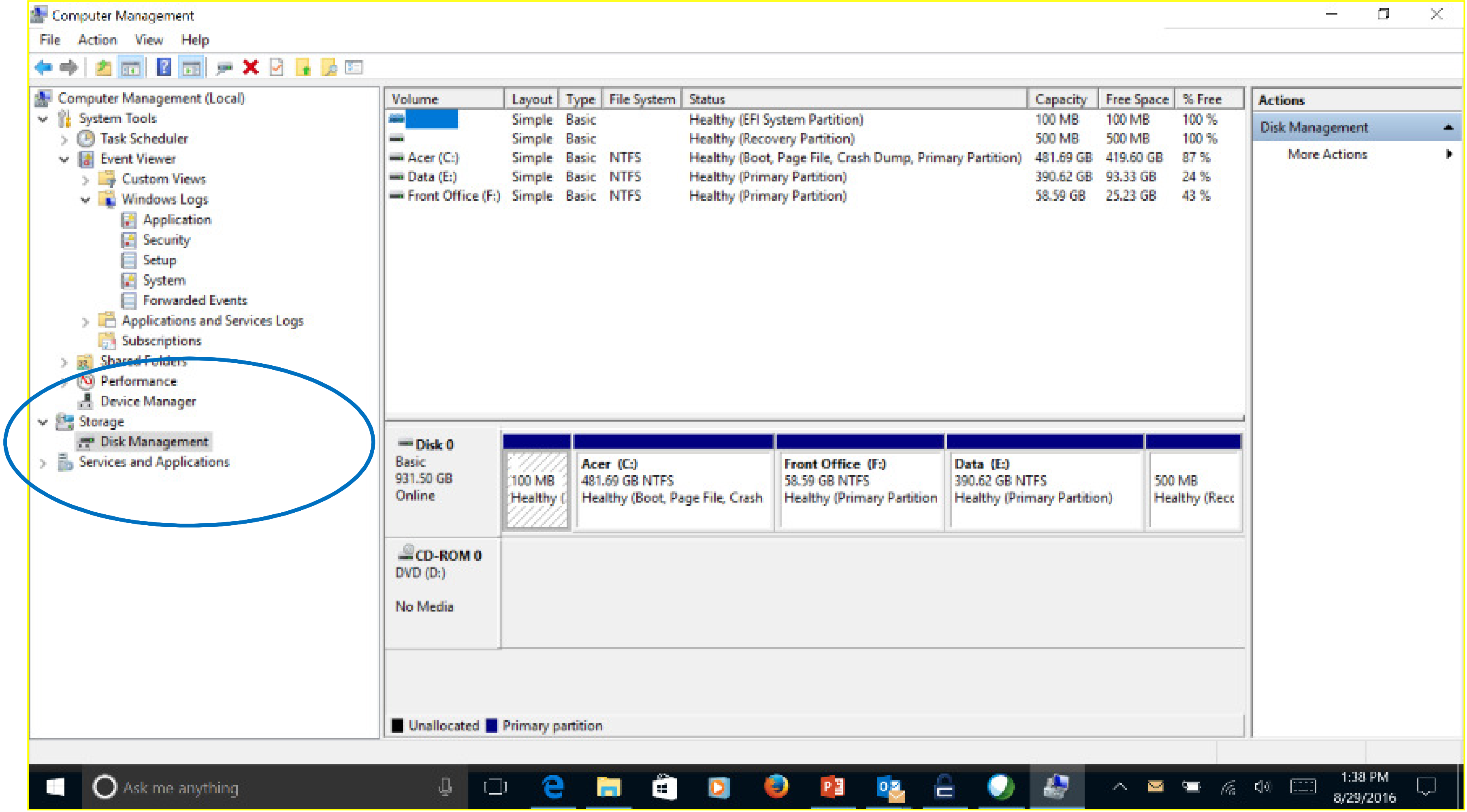
Physical Memory (K)	
Total	12,446,300
Available	7,862,520
Cache WS	0
Kernel WS	0
Driver WS	32,764

Kernel Memory (K)	
Paged WS	524,532
Paged Virtual	557,268
Paged Limit	no symbols
Nonpaged	282,960
Nonpaged Limit	no symbols

Paging	
Page Fault Delta	2,157
Page Read Delta	0
Paging File Write Delta	0
Mapped File Write Delta	0

Paging Lists (K)	
Zeroed	160,132
Free	20
Modified	112,956
ModifiedNoWrite	0
Standby	7,702,368
Priority 0	420
Priority 1	2,500
Priority 2	1,414,472
Priority 3	119,920
Priority 4	374,596
Priority 5	5,632,664
Priority 6	0
Priority 7	157,796
PageFileModified	112,924

DETECTION PROCEDURES SERVER EXAMPLE 1



Volume	Layout	Type	File System	Status	Capacity	Free Space	% Free
	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 0
Basic
931.50 GB
Online

100 MB
Healthy (

Acer (C:)
481.69 GB NTFS
Healthy (Boot, Page File, Crash

Front Office (F:)
58.59 GB NTFS
Healthy (Primary Partition

Data (E:)
390.62 GB NTFS
Healthy (Primary Partition)

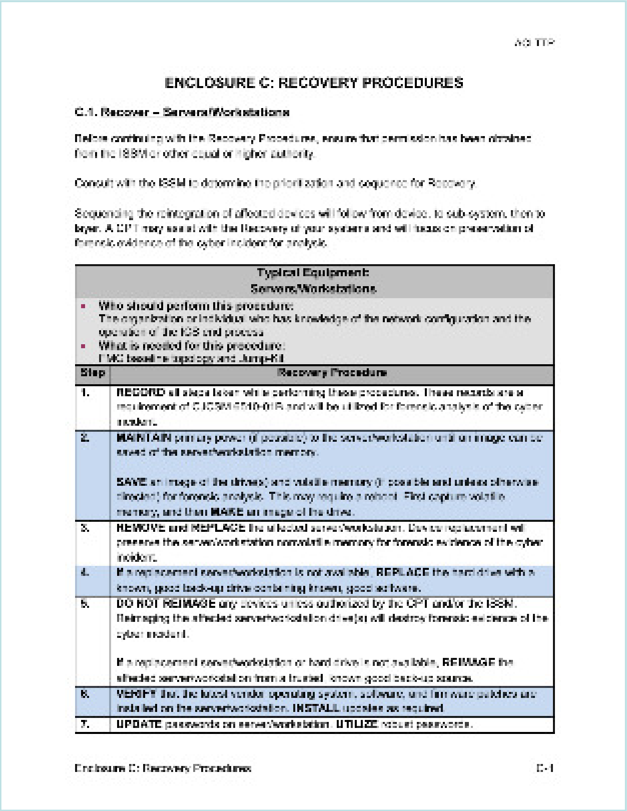
500 MB
Healthy (Recc

CD-ROM 0
DVD (D:)

No Media

■ Unallocated ■ Primary partition

ENCLOSURE C: RECOVERY PROCEDURES



ACI TTP

ENCLOSURE C: RECOVERY PROCEDURES

C.1. Recover – Servers/Workstations

Before continuing with the Recovery Procedures, ensure that permission has been obtained from the ISSM or other equal or higher authority.

Consult with the ISSM to determine the prioritization and sequence for Recovery.

Sequencing the reintegration of affected devices will follow from device, to sub-system, then to layer. A CPT may assist with the Recovery of your systems and will focus on preservation of forensic evidence of the cyber incident for analysis.

Typical Equipment:
Servers/Workstations

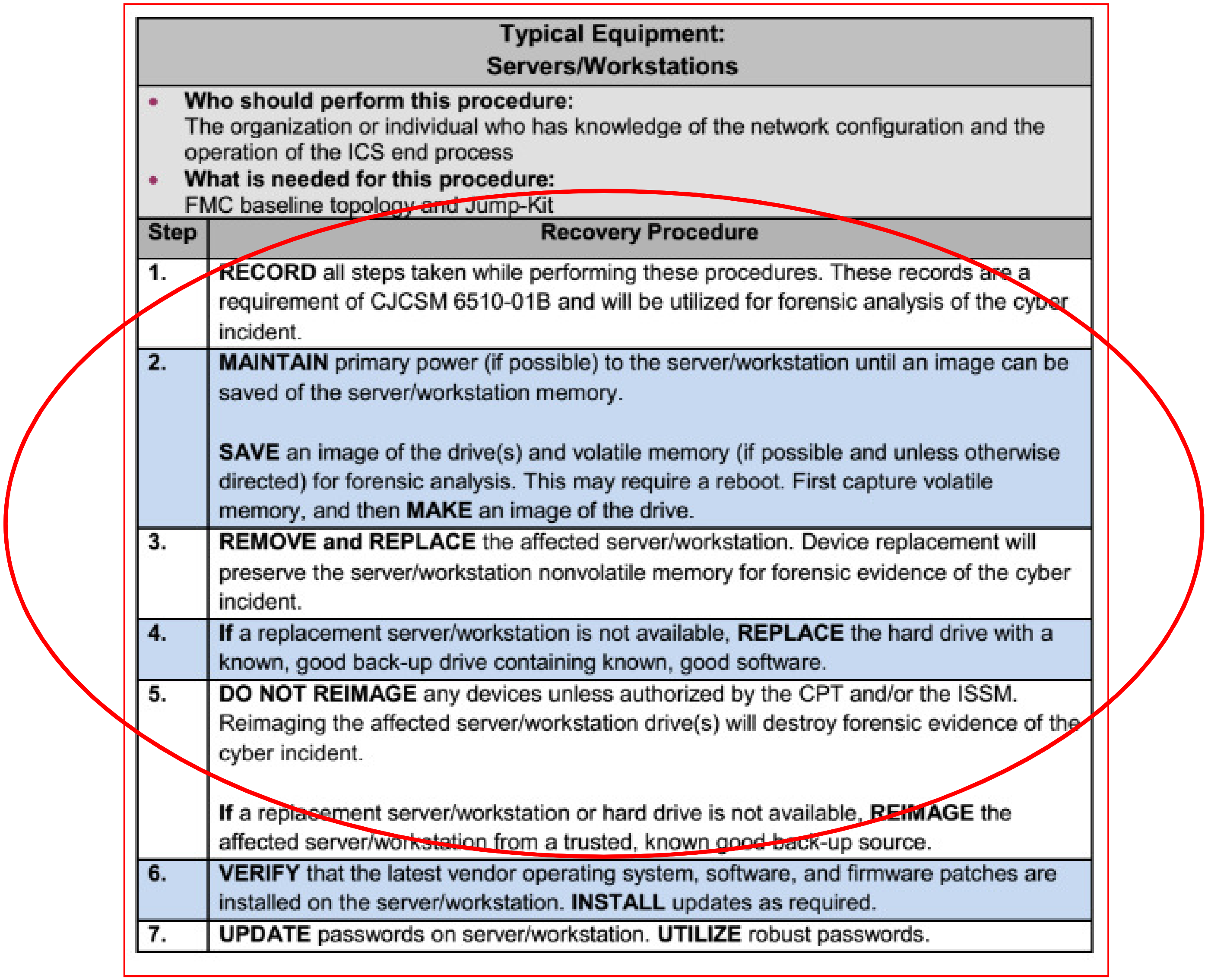
- **Who should perform this procedure:**
  The organization or individual who has knowledge of the network configuration and the operation of the ICS and process
- **What is needed for this procedure:**
  FMC baseline topology and Jump-Kit

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 C: Recovery Procedures C-1

C.1 Recover – Servers/Workstations
C.2 Recover – Routers/Switches/Modems/Printers
C.3 Recover – RTU, MTU, and PLC
C.4 Recover – Intelligent Electronic Devices (IEDs)
C.5 Recover – Human-Machine Interface (HMI)
C.6 Recover – Firewalls
C.7 Recover – Media Converters (Serial/Fiber Converter)

RECOVERY PROCEDURES SERVER EXAMPLE 1

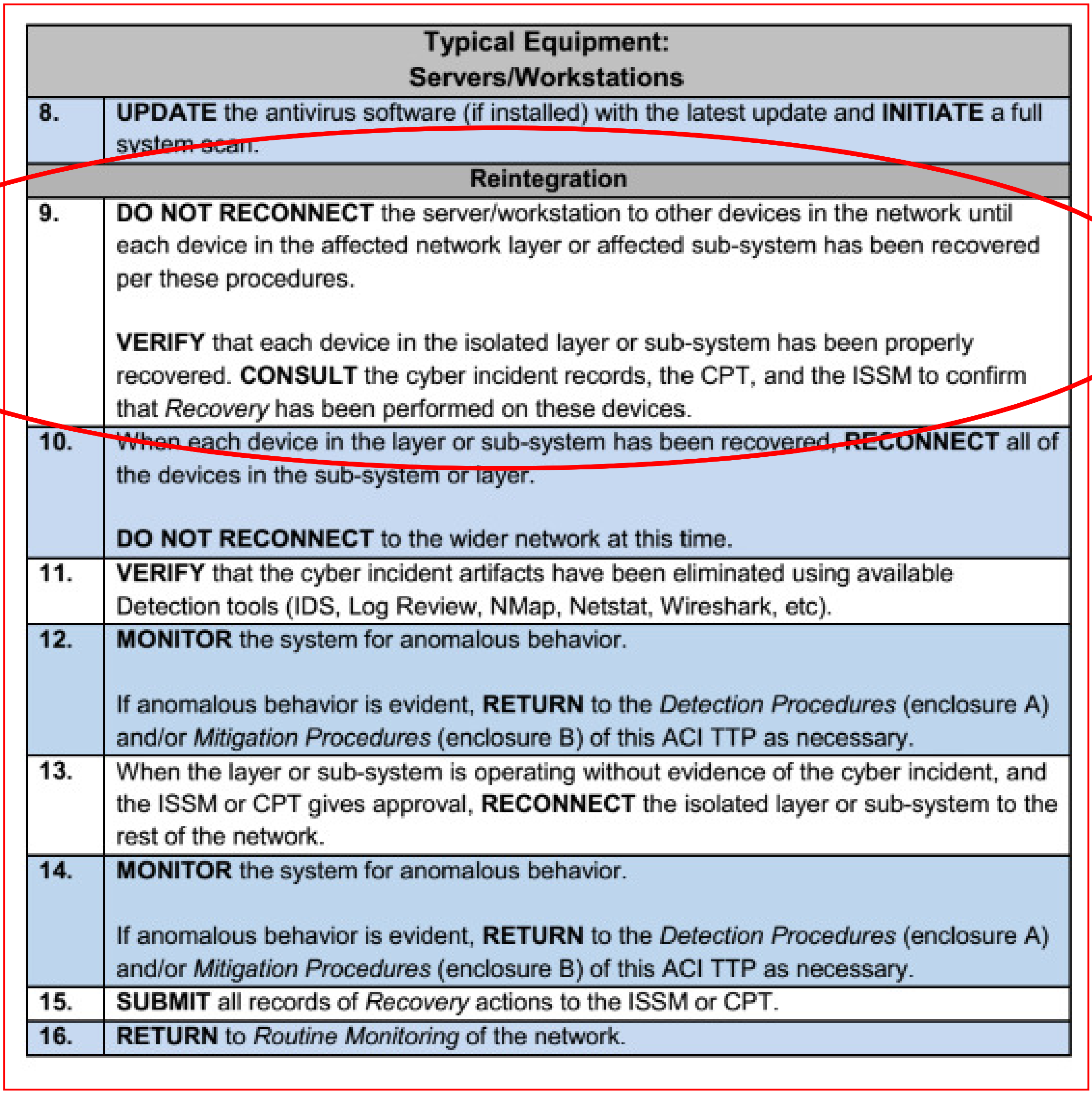


Typical Equipment:
Servers/Workstations

- **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.

RECOVERY PROCEDURES SERVER EXAMPLE 1

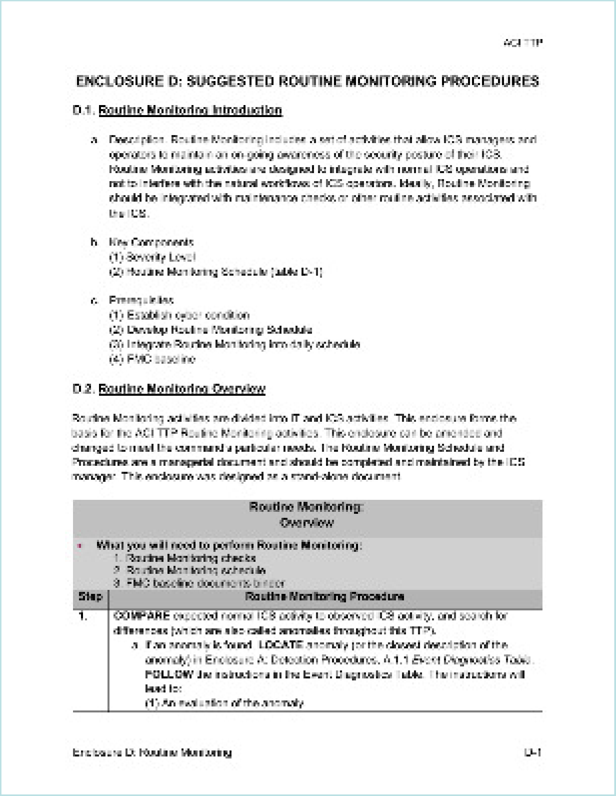


Typical Equipment: Servers/Workstations	
8.	**UPDATE** the antivirus software (if installed) with the latest update and **INITIATE** a full system scan.
Reintegration	
9.	**DO NOT RECONNECT** the server/workstation to other devices in the network until each device in the affected network layer or affected sub-system has been recovered per these procedures. **VERIFY** that each device in the isolated layer or sub-system has been properly recovered. **CONSULT** the cyber incident records, the CPT, and the ISSM to confirm that *Recovery* has been performed on these devices.
10.	When each device in the layer or sub-system has been recovered, **RECONNECT** all of the devices in the sub-system or layer. **DO NOT RECONNECT** to the wider network at this time.
11.	**VERIFY** that the cyber incident artifacts have been eliminated using available Detection tools (IDS, Log Review, NMap, Netstat, Wireshark, etc).
12.	**MONITOR** the system for anomalous behavior. If anomalous behavior is evident, **RETURN** to the *Detection Procedures* (enclosure A) and/or *Mitigation Procedures* (enclosure B) of this ACI TTP as necessary.
13.	When the layer or sub-system is operating without evidence of the cyber incident, and the ISSM or CPT gives approval, **RECONNECT** the isolated layer or sub-system to the rest of the network.
14.	**MONITOR** the system for anomalous behavior. If anomalous behavior is evident, **RETURN** to the *Detection Procedures* (enclosure A) and/or *Mitigation Procedures* (enclosure B) of this ACI TTP as necessary.
15.	**SUBMIT** all records of *Recovery* actions to the ISSM or CPT.
16.	**RETURN** to *Routine Monitoring* of the network.

Chapter 4 – Recovery Concepts (cont)

(3) Cyber Issues. Critical to effective Recovery reintegration is ensuring that newly recovered devices will not be re-infected. The best way to avoid this problem is to verify that each device on the network is clean of any cyber incident remnants. **All devices in the network should be replaced or re-flashed with known, good firm/software to provide confidence that re-infection will not occur.** If expedience for Recovery of the network takes precedence over this conservative rationale, a risk analysis should be performed in consultation with the ISSM and/or your chain of command. The risk analysis should consider the likelihood of re-infection of newly recovered devices when reconnecting to devices in the network.

ENCLOSURE D: MONITORING PROCEDURES



ACI TTP

ENCLOSURE D: SUGGESTED ROUTINE MONITORING PROCEDURES

D.1. Routine Monitoring Introduction

a. Description. Routine Monitoring includes a set of activities that allow ICS managers and operators to maintain an on-going awareness of the security posture of their ICS. Routine Monitoring activities are designed to integrate with normal ICS operations and not to interfere with the natural workflows of ICS operators. Ideally, Routine Monitoring should be integrated with maintenance checks or other routine activities associated with the ICS.

b. Key Components
(1) Severity Level
(2) Routine Monitoring Schedule (table D-1)

c. Prerequisites
(1) Establish cyber condition
(2) Develop Routine Monitoring Schedule
(3) Integrate Routine Monitoring into daily schedule
(4) FMC baseline

D.2. Routine Monitoring Overview

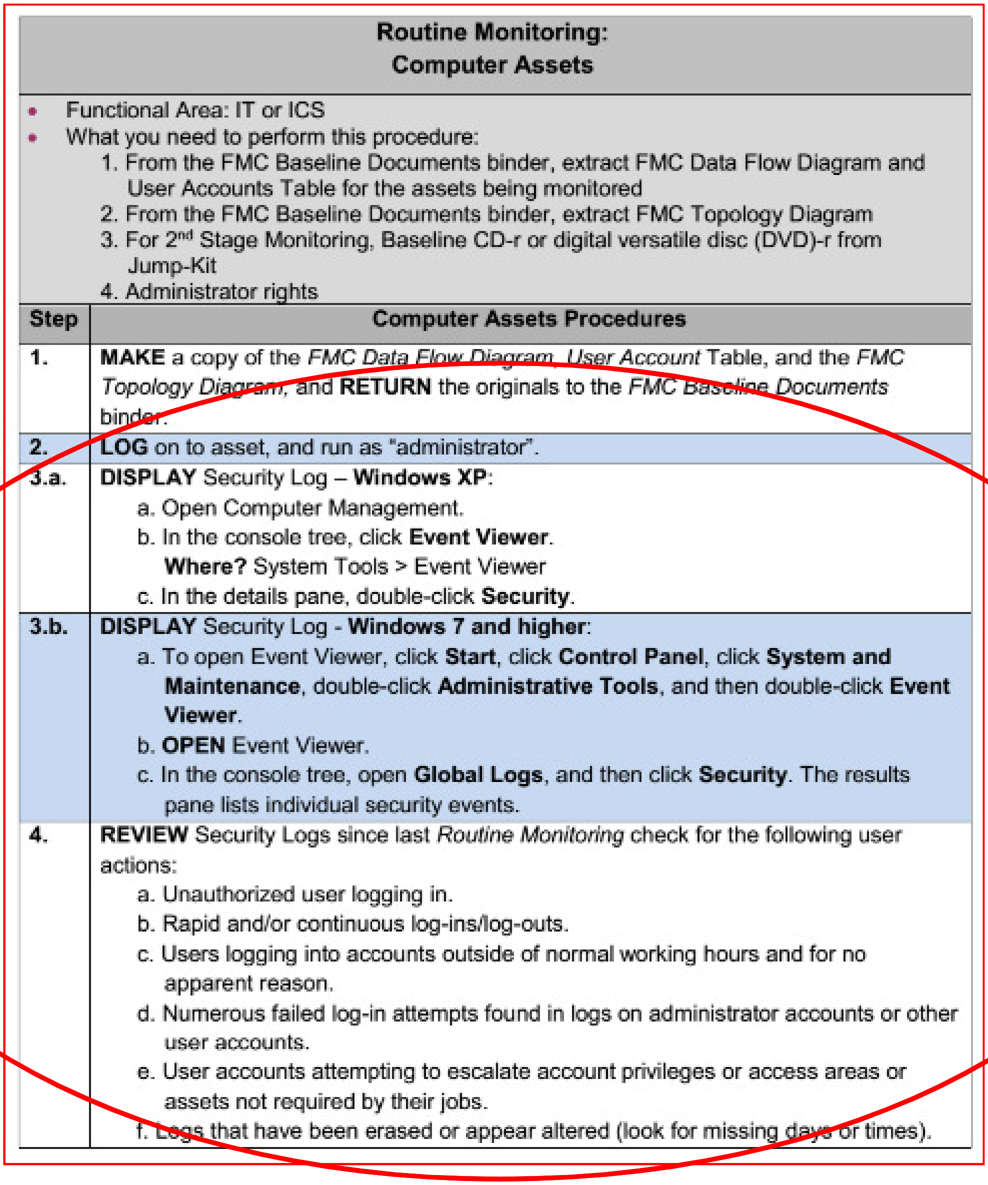
Routine Monitoring activities are divided into IT and ICS activities. This enclosure forms the basis for the ACI TTP Routine Monitoring activities. This enclosure can be amended and changed to meet the command's particular needs. The Routine Monitoring Schedule and Procedures are a managerial document and should be completed and maintained by the ICS manager. This enclosure was designed as a stand-alone document.

Routine Monitoring: Overview	
▪ What you will need to perform Routine Monitoring: 1. Routine Monitoring checks 2. Routine Monitoring schedule 3. FMC baseline documents binder	
Step	**Routine Monitoring Procedure**
1.	**COMPARE** expected normal ICS activity to observed ICS activity, and search for differences (which are also called anomalies throughout this TTP). a. If an anomaly is found, **LOCATE** anomaly (or the closest description of the anomaly) in Enclosure A: Detection Procedures, A.1.1 *Event Diagnostics Table*. **FOLLOW** the instructions in the Event Diagnostics Table. The instructions will lead to: (1) An evaluation of the anomaly

Enclosure D: Routine Monitoring D-1

D.1 Routine Monitoring Introduction
D.2 Routine Monitoring Overview
D.3 Routine Monitoring: Security Events and IDS Alert Check
D.4 Routine Monitoring: Security Events and Firewall Log Check
D.5 Routine Monitoring: Computer Assets
D.6 Routine Monitoring: Network Data Flow
D.7 Routine Monitoring: Synchronicity Check

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 G: FORENSICS

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.

b. Key Components

(1) Volatile memory
(2) Non-volatile data
(3) Collection
(4) Documentation
(5) Notifications

c. Prerequisites

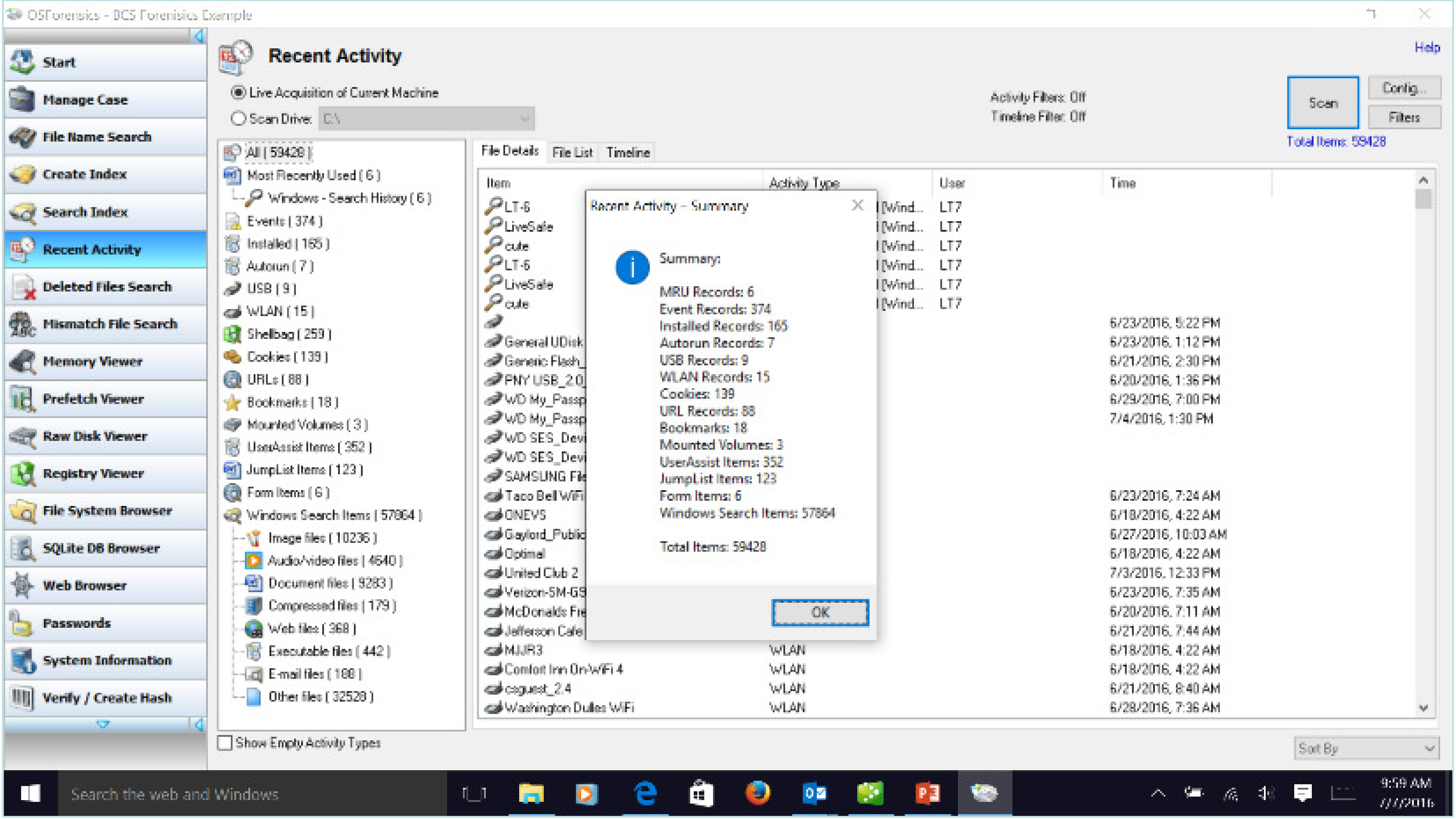
(1) Administrative tools for acquisition
(2) Storage devices to capture and transport evidence

G.3. Data Collection Tools

G.3. Data Collection Tools

- Mandiant Redline
- Mandiant Memoryze
- Microsoft SysInternals
- Microsoft Windows system utilities
- Linux system utilities
- Glasswire
- OSForensics
- RegRipper
- Belarc

OS Forensics Recent Activity



Recent Activity

● Live Acquisition of Current Machine

○ Scan Drive: C:\

Activity Filters: Off
Timeline Filter: Off

Total Items: 59428

- All (59428)
- Most Recently Used (6)
  - Windows - Search History (6)
- Events (374)
- Installed (165)
- Autorun (7)
- USB (9)
- WLAN (15)
- Shellbag (259)
- Cookies (139)
- URLs (88)
- Bookmarks (18)
- Mounted Volumes (3)
- UserAssist Items (352)
- JumpList Items (123)
- Form Items (6)
- Windows Search Items (57864)
  - Image files (10236)
  - Audio/video files (4640)
  - Document files (9283)
  - Compressed files (179)
  - Web files (368)
  - Executable files (442)
  - E-mail files (188)
  - Other files (32528)

□ Show Empty Activity Types

Item	Activity Type	User	Time
LT-6	[Wind...	LT7	
LiveSale	[Wind...	LT7	
cute	[Wind...	LT7	
LT-6	[Wind...	LT7	
LiveSale	[Wind...	LT7	
cute	[Wind...	LT7	
			6/23/2016, 5:22 PM
General UDisk			6/23/2016, 1:12 PM
Generic Flash_			6/21/2016, 2:30 PM
PNY USB_2.0			6/20/2016, 1:36 PM
WD My_Passp			6/29/2016, 7:00 PM
WD My_Passp			7/4/2016, 1:30 PM
WD SES_Devi			
WD SES_Devi			
SAMSUNG File			
Taco Bell WiFi			6/23/2016, 7:24 AM
ONEVS			6/18/2016, 4:22 AM
Gaylord_Public			6/27/2016, 10:03 AM
Optimal			6/18/2016, 4:22 AM
United Club 2			7/3/2016, 12:33 PM
Verizon-SM-GS			6/23/2016, 7:35 AM
McDonalds Fre			6/20/2016, 7:11 AM
Jefferson Cafe			6/21/2016, 7:44 AM
MJJR3	WLAN		6/18/2016, 4:22 AM
Comfort Inn On-WiFi 4	WLAN		6/18/2016, 4:22 AM
csguest_2.4	WLAN		6/21/2016, 8:40 AM
Washington Dulles WiFi	WLAN		6/28/2016, 7:36 AM

Recent Activity – Summary

Summary:

MRU Records: 6
Event Records: 374
Installed Records: 165
Autorun Records: 7
USB Records: 9
WLAN Records: 15
Cookies: 139
URL Records: 88
Bookmarks: 18
Mounted Volumes: 3
UserAssist Items: 352
JumpList Items: 123
Form Items: 6
Windows Search Items: 57864

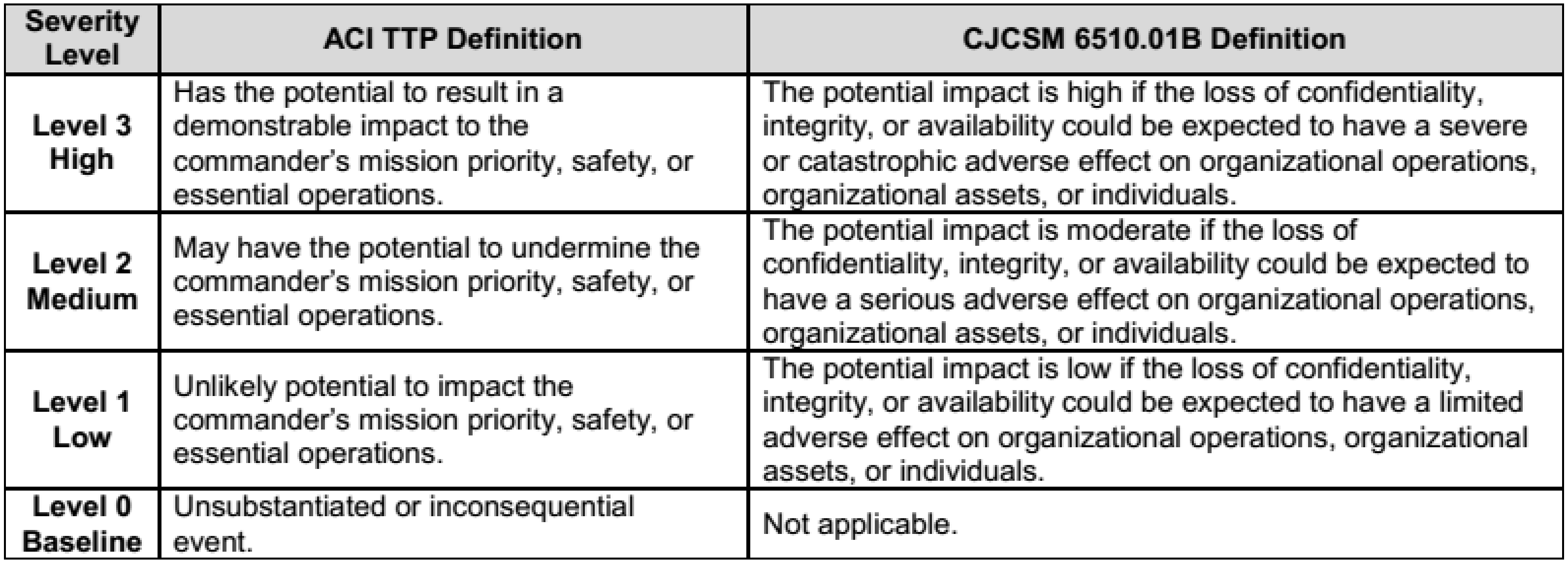
Total Items: 59428

OK

I.3. INCIDENT SEVERITY LEVELS

I.3. Incident Severity Levels

The Severity Level Scale is **a range between 3 and 0, from the least severity to the greatest severity,** respectively. Table I-1 provides the ACI TTP definitions as well as the CJCSM 6510.01B definitions.



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

Table I-1: Incident Severity Levels

Questions

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

Daryl Haegley
President, DRH Consulting
Cell: 757-303-3287
E-mail: dhaegley@gmail.com