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

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


Federal Standards

- OMB 21st Century Digital Strategy – requires movement to Cloud and Web Services

Committee for National Security Systems


DoD Policy

- DoDI 8500.01 Cybersecurity – replaces DIACAP with NIST Risk Management Framework (expected release Feb 2013)
- CIO IT Modernization Strategy and Roadmap – requires data center and server consolidation
- CIO Mobile Device Strategy – instructs implementation of mobile devices on DoD networks
- CIO Cloud Computing Strategy – requires DoD to move to Cloud and Web Based Services

Unified Facility Criteria – multiple UFC’s will need to be updated

Engineering Technical Letters – multiple ETLS will need to be updated

Shodan Site = Locates CS

DoD has many CS systems directly connected to internet with no protection, http
OT IP Controllers are in **Everything**

![Diagram showing various applications of OT IP Controllers](image)

*Same Commercial Device Installed Across DoD Enterprise; PIT & PIT Systems*
Broader Cybersecurity Efforts
“8 Star Memo”

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 B. GORTNEY
Admiral, U.S. Navy
Commander, U.S. Northern Command

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.
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

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

**McAfee Nessus Retina Forcepoint**

**Client Side Attacks**
- Sophia GrassMarlin Others?

**Server Side Attacks**

**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
TTP Website Access WBDG and RMF KS

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

http://www.wbdg.org/resources/cybersecurity.php
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 CIC supporting documentation. This effort should result in the c package. The required artifacts are determined by the system 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 Manager
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

(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.

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.
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

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 assist 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.
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

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

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 organization.

<table>
<thead>
<tr>
<th>Date: 6/15/16</th>
<th>Operator: Joe Operator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>Asset</td>
</tr>
<tr>
<td>830</td>
<td>Primary HMI</td>
</tr>
<tr>
<td>845</td>
<td>OPC Server</td>
</tr>
<tr>
<td>900</td>
<td></td>
</tr>
<tr>
<td>915</td>
<td>Primary HMI, OPC Server</td>
</tr>
</tbody>
</table>
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
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.
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 reimagine 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.
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

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

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

### 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
## A.1.1 Event Diagnostics Table

<table>
<thead>
<tr>
<th>Section</th>
<th>Event</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Notification</strong></td>
<td>A.2.1</td>
<td>Notifications</td>
<td>Cyber event notifications are issued by a variety of entities, including USCYBERCOM, ICS-CERT, or the command directives.</td>
</tr>
<tr>
<td><strong>Server/Workstation Anomalies</strong></td>
<td>A.2.2</td>
<td>Log File Check: Unusual Account Usage/Activity</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>A.2.3</td>
<td>Irregular Process Found</td>
<td>On any computer-based server, workstation(s), including SCADA equipment, an irregular process was found.</td>
</tr>
<tr>
<td></td>
<td>A.2.4</td>
<td>Suspicious Software/ Configurations</td>
<td>Suspicious software and/or configurations were Detected on a server or workstation.</td>
</tr>
<tr>
<td></td>
<td>A.2.5</td>
<td>Irregular Audit Log Entry (or Missing Audit Log)</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>A.2.6</td>
<td>Unusual System Behavior</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>A.2.7</td>
<td>Asset is Scanning Other Network Assets</td>
<td>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.</td>
</tr>
</tbody>
</table>
# 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Procedures</th>
</tr>
</thead>
</table>
| **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:  
  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**. |
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

<table>
<thead>
<tr>
<th>Step</th>
<th>Procedures</th>
</tr>
</thead>
</table>
| 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.3.2.3 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
DETECTION PROCEDURES SERVER EXAMPLE 1
ENCLOSURE C: RECOVERY PROCEDURES

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Recovery Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td><strong>RECORD</strong> 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.</td>
</tr>
<tr>
<td>2.</td>
<td><strong>MAINTAIN</strong> primary power (if possible) to the server/workstation until an image can be saved of the server/workstation memory. <strong>SAVE</strong> 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 <strong>MAKE</strong> an image of the drive.</td>
</tr>
<tr>
<td>3.</td>
<td><strong>REMOVE</strong> and <strong>REPLACE</strong> the affected server/workstation. Device replacement will preserve the server/workstation nonvolatile memory for forensic evidence of the cyber incident.</td>
</tr>
<tr>
<td>4.</td>
<td><strong>If a</strong> replacement server/workstation is not available, <strong>REPLACE</strong> the hard drive with a known, good back-up drive containing known, good software.</td>
</tr>
<tr>
<td>5.</td>
<td><strong>DO NOT REIMAGE</strong> 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, <strong>REIMAGE</strong> the affected server/workstation from a trusted, known good back-up source.</td>
</tr>
<tr>
<td>6.</td>
<td><strong>VERIFY</strong> that the latest vendor operating system, software, and firmware patches are installed on the server/workstation. <strong>INSTALL</strong> updates as required.</td>
</tr>
<tr>
<td>7.</td>
<td><strong>UPDATE</strong> passwords on server/workstation. <strong>UTILIZE</strong> robust passwords.</td>
</tr>
</tbody>
</table>

**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
## RECOVERY PROCEDURES SERVER EXAMPLE 1

<table>
<thead>
<tr>
<th>Typical Equipment: Servers/Workstations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>8.</strong> UPDATE the antivirus software (if installed) with the latest update and INITIATE a full system scan.</td>
</tr>
</tbody>
</table>

### 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. |
(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.
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

<table>
<thead>
<tr>
<th>Step</th>
<th>Computer Assets Procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td><strong>MAKE</strong> a copy of the FMC Data Flow Diagram, User Account Table, and the FMC Topology Diagram, and <strong>RETURN</strong> the originals to the FMC Baseline Documents binder.</td>
</tr>
<tr>
<td>2.</td>
<td><strong>LOG</strong> on to asset, and run as &quot;administrator&quot;.</td>
</tr>
</tbody>
</table>
| 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: 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

- Mandiant Redline
- Mandiant Memoryze
- Microsoft SysInternals
- Microsoft Windows system utilities
- Linux system utilities
- Glasswire
- OSForensics
- RegRipper
- Belarc
OS Forensics Recent Activity
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.

<table>
<thead>
<tr>
<th>Severity Level</th>
<th>ACI TTP Definition</th>
<th>CJCSM 6510.01B Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 3 High</td>
<td>Has the potential to result in a demonstrable impact to the commander’s mission priority, safety, or essential operations.</td>
<td>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.</td>
</tr>
<tr>
<td>Level 2 Medium</td>
<td>May have the potential to undermine the commander’s mission priority, safety, or essential operations.</td>
<td>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.</td>
</tr>
<tr>
<td>Level 1 Low</td>
<td>Unlikely potential to impact the commander’s mission priority, safety, or essential operations.</td>
<td>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.</td>
</tr>
<tr>
<td>Level 0 Baseline</td>
<td>Unsubstantiated or inconsequential event.</td>
<td>Not applicable.</td>
</tr>
</tbody>
</table>

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