



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

Revision 2, March 2018

This page intentionally left blank.



**DEPARTMENT OF DEFENSE
UNITED STATES CYBER COMMAND**
9800 SAVAGE ROAD, SUITE 6171
FORT GEORGE G. MEADE, MARYLAND 20755

Reply to:
Commander

AUG 10 2016

MEMORANDUM FOR RECORD

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

1. Around the globe, ICS enable our military to strike quickly, respond to distant crises, and achieve efficiency in warfighting. To secure, operate, and defend our ICS, I endorse the United States Cyber Command (USCYBERCOM) ACI TTP. It includes tested and verified practices of experts across the DoD who understand the threat to these vital systems.
2. The purpose of this ACI TTP is to help DoD ICS practitioners effectively operate their systems to thwart compromise and attacks. It is intended to provide procedures that enable ICS managers to detect advanced cyber attacks, mitigate the effects of those attacks, and recover their networks following an attack. It also supports the USCYBERCOM mission in deterring and defeating strategic threats to United States interests and infrastructure while ensuring DoD mission assurance.
3. I encourage users and managers of ICS throughout DoD and supporting organizations to apply the lessons and practices in the ACI TTP to help detect, mitigate, and recover from attacks on our systems. It is no coincidence that our adversaries spend time and effort gaining access into our critical infrastructures. The ACI TTP takes a vital and necessary step towards protecting ICS, thereby enabling DoD warfighting missions.



MICHAEL S. ROGERS
Admiral, U.S. Navy
Commander

This page intentionally left blank.

Distribution

This product results from a collaborative effort by United States Cyber Command (USCYBERCOM) which sponsored and supported the Joint Base Architecture for Secure Industrial Control Systems Joint Test (also commonly referred to as “J-BASICS JT”) and the Joint Test and Evaluation (JT&E) Program under the Director, Operational Test and Evaluation, Office of the Secretary of Defense. The JT&E Program seeks nominations from Services, combatant commands, and national agencies for projects that develop test products to resolve joint operational problems.

The objective of the JT&E Program is to find ways for warfighters to improve mission performance with current equipment, organizations, and doctrine by developing test products that resolve joint operational problems through process improvements. Please visit <https://www.jte.osd.mil> (CAC required) for additional information on the JT&E Program.

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited.

This page intentionally left blank.

Revisions

Version	Date	Revision	Comments
1	January 1, 2016	0	Initial Distribution
1	January 20, 2017	1	Created new section A.3.2.17 and Appendix E. Updated Chapter 1, and sections A.2, A.3.2.6, and D.5. Updated tables A.3.1 and D-1. Added “Distribution Statement A”.
1	March 22, 2018	2	Updates to Enclosure A, Enclosure D, Enclosure E, Enclosure G, and Appendix E including: Malware process detection Malware process injection Unauthorized usage - admin tools/utilities File detection Internal network traffic anomalies External network traffic anomalies Additional references to SysInternals utilities Update outdated references Other misc. items

ACI TTP Revision 2 Summary of Changes

Executive Summary

Over the past year, it has become evident that malware targeting Industrial Control Systems (ICS) environments has begun to evolve towards advanced ICS malware suites. These malware suites may be composed of multiple modules with each module specialized to a targeted task. This modularity may indicate a move towards more sophisticated development processes as well as possible plans by malware developers for future reuse, extension, and updates to code. This apparent evolution of malware development processes is in line with malware development seen for non-ICS environments.

In response to the evolution of the malware development processes (and malware's increasing complexity), the following concept areas have been added/updated across a number of sections of the Advanced Cyber Industrial Tactics, Techniques, Procedures (ACI TTP):

- 1) malware process detection
- 2) unauthorized usage - admin tools/utilities
- 3) file detection
- 4) internal network traffic anomalies
- 5) external network traffic anomalies.

These updates address concerns arising from the advent of advanced ICS malware suites. Updates have also been made to Appendix E, which contains a greater amount of detail (or additional options) when using the updated detection methods.

Please note that there is a predominance of Microsoft Windows focused recommendations in this guide. Although specific ICS hardware may or may not operate on Windows or Embedded Windows, the software that is used to administer this hardware is most likely running on Windows. As more ICS systems begin to use other operating systems, this guide will be updated. Some of the included guidance is not Operating System (OS) specific but is more procedure oriented. In many cases, the Windows focused guidance and concepts discussed will often apply to other OSs as well (with minor adjustments to command line syntax and/or file names/locations).

In some cases, multiple methods are given to detect the same type of malicious activity. Some of these methods require software not included by default in a Windows installation (e.g. Microsoft SysInternals Utilities). These utilities will be identified with blue font. If the environment does not allow for these utilities, use one of the default Windows utilities options instead.

The updates to the ACI TTP included the addition of the following procedures:

- **Adjust Windows Policy to log use of command shell.**

Malware may attempt to manipulate a system by executing commands from an operating system's "shell" or command line. By default, opening of a Microsoft Windows command shell does not generate an event log entry; this makes monitoring for this activity difficult. It is possible to adjust Windows policy (in Windows 7 and later) to log this information to the Windows event log as Security event ID 4688.

- **Detect unknown processes, DLLs, EXEs, or threads.**
Malware may attempt to execute malicious processes on a targeted system. It is important to detect the appearance of these processes. Review currently running processes against baseline processes.
- **Detect malware manipulation of legitimate processes.**
Malware may stop or kill, and then start legitimate processes in order to manipulate a system. Since “ungraceful” process stops/kills are not usually logged, it may be easier to use methods to detect subsequent/or recent process starts/restarts. Recent process starts (outside of normal maintenance windows) for long running systems may indicate that malicious manipulation has occurred and this could warrant further review.
- **Detect unusual/unauthorized attachment, insertion, and/or removal to/from processes (e.g. process injection).**
Malware may attempt to hide its activities from antivirus software by attaching or inserting itself into a legitimate process and/or service (rather than creating its own process service). Reviewing the legitimate processes and/or services in detail could identify these possible malicious attachments or insertions.
- **Detect malware overwrite of an existing application or Windows service’s “image path”.**
Overwrite of the image path in the Windows Registry can be used to establish malware persistence. Malware may sometimes attempt to overwrite the image paths (file locations) of legitimate files in the Windows Registry in order to point to the location of a malicious file. In doing this, the malware may be able to redirect the OS (or user) to execute the malicious file instead of the legitimate one originally intended by the OS (or user).
- **Detect malware manipulation of serial ports/connected serial devices.**
ICS focused malware may attempt to manipulate serial connections available on a target host (if found) in order to target connected ICS hardware. It may be beneficial to evaluate the configurations and status of a host’s serial ports. The Window’s *mode* command is used to review these configurations and the user can then compare the configuration information to baseline. Additional utilities (discussed in Appendix E) can assist with this review.
- **Network Card - Promiscuous mode detection.**
Network cards in Promiscuous mode will attempt to “listen” to all traffic on the local subnet (rather than only the traffic intended for the host). Malware could possibly use this mode to gather sensitive information.
- **Detect “Wiper” type malware activity.**
Detect malicious overwrite of ICS file types and/or configuration files. Review both local drives and mapped network drives for unexpected changes. Note: it is important to identify and review file-types associated with your environment’s specific ICS products.

- **Detect unexpected encrypted or high entropy files.**
The Microsoft SysInternals [sigcheck](#) utility can show the entropy level of a file and possibly identify encrypted files. Unexpected files with high entropy may warrant further review. Note: It is recommended to perform this check selectively on only unexpected or suspicious files (as unencrypted compressed files may cause false positives).
- **Malicious File Detection – via file hash**
The Microsoft SysInternals [sigcheck](#) utility can run a cryptographic hash of a file (e.g. md5, sha, etc.). This can be used to compare a suspicious file against known bad files (i.e. either from reporting or from online services such as VirusTotal).
- **Detect Privilege escalation**
Malware may attempt to gain privileges on an OS (i.e. from a standard user to administrator) in order to execute tasks that require administrative privileges.
 - Detect Windows Scheduler based or similar attacks:
 - Unauthorized usage of: AT, WinAT, RunAs functionality
 - Review Windows Event Log for specific eventIDs and determine if the event(s) were authorized.
 - Review accounts and permissions to detect unauthorized additions to privileged groups/accounts: Display a list of users on the local machine and compare output to the baseline.
- **Detect unauthorized usage of Windows admin tools and utilities (SysInternals, PowerShell, etc.)**
Malware may attempt to use administrative or system utilities in order to execute tasks or gather information. Monitor for unauthorized use of these utilities.

PREFACE

Since the 1970s, industrial control systems (ICS) networks have provided safe and efficient monitoring and use in all sectors of critical infrastructure. Department of Defense (DoD) facilities around the world are heavily dependent on ICS. ICS networks allow operational systems to be remotely controlled to support the warfighter in various mission spaces.

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.

To better defend DoD ICS, United States Cyber Command (USCYBERCOM) sponsored and supported the Joint Base Architecture for Secure Industrial Control Systems (J-BASICS) Joint Test (JT). This JT involved the development, test, evaluation, and refinement of the Advanced Cyber Industrial Control System (ACI) TTP for DoD ICS. This ACI TTP is designed to enable managers of ICS networks to *Detect, Mitigate, and Recover* from nation-state-level cyber attacks (strategic, deliberate, well-trained, and funded attacks to support greater strategic objectives).

In his Statement for the Record to the Senate Select Committee on Intelligence in March 2013, the United States Director of National Intelligence, James R. Clapper, describes nation-state-level attacks as being of two types: cyber espionage and cyber attacks. Director Clapper further describes cyber threats as follows:

A cyber attack is a non-kinetic offensive operation intended to create physical effects or to manipulate, disrupt, or delete data. It might range from a denial-of-service operation that temporarily prevents access to a website, to an attack on a power turbine that causes physical damage and an outage lasting for days. Cyber espionage refers to intrusions into networks to access sensitive diplomatic, military, or economic information.

To further his point, Director Clapper emphasized that there is an increasing risk to critical infrastructure, “resulting in long-term, wide-scale disruption of services, such as regional power outages”. It is in the shadow of these threats that this ACI TTP was developed.

This page intentionally left blank.

TABLE OF CONTENTS

OVERVIEW

CHAPTER 1: ACI TTP OVERVIEW.....	1-1
1. Purpose.....	1-1
2. Scope.....	1-1
3. How to Use These TTP	1-1
4. Navigating Detection, Mitigation, and Recovery Procedures	1-3
5. Maintaining Operational Resilience	1-4
6. CIA Triad.....	1-5
7. Operational Security Log	1-5
CHAPTER 2: ACI TTP DETECTION CONCEPTS.....	2-1
1. Detection Introduction	2-1
2. Detection Overview	2-1
3. Detection Process	2-2
CHAPTER 3: ACI TTP MITIGATION CONCEPTS	3-1
1. Mitigation Introduction	3-1
2. Mitigation Overview	3-2
3. Mitigation Process	3-2
CHAPTER 4: ACI TTP RECOVERY CONCEPTS	4-1
1. Recovery Introduction	4-1
2. Recovery Overview	4-1
3. Recovery Process	4-2
4. Sequences and Reintegration for Recovery	4-3
THREAT-RESPONSE PROCEDURES	
ENCLOSURE A: DETECTION PROCEDURES	A-1
A.1 Event Diagnostics	A-1
A.1.1 Event Diagnostics Table.....	A-1
A.2 Event Diagnostic Procedures	A-5
A.3 Integrity Checks	A-35
A.3.1 Integrity Checks Table.....	A-35
A.3.2 Integrity Checks Procedures	A-36
ENCLOSURE B: MITIGATION PROCEDURES	B-1
B.1 Mitigation Segmentation.....	B-1
B.2 IT/Network Assets.....	B-2
B.3 ICS Control Device Mitigation	B-3

ENCLOSURE C: RECOVERY PROCEDURES	C-1
C.1 Recover – Servers/Workstations.....	C-1
C.2 Recover – Routers/Switches/Modems/Printers	C-3
C.3 Recover – RTU, MTU, and PLC.....	C-5
C.4 Recover – Intelligent Electronic Devices (IEDs)	C-7
C.5 Recover – Human-Machine Interface (HMI).....	C-9
C.6 Recover – Firewalls	C-11
C.7 Recover – Media Converters (Serial/Fiber Converter)	C-13

REFERENCE MATERIALS

ENCLOSURE D: SUGGESTED ROUTINE MONITORING PROCEDURES	D-1
D.1 Routine Monitoring Introduction	D-1
D.2 Routine Monitoring Overview	D-1
D.3 Routine Monitoring: Security Events and IDS Alert Check	D-4
D.4 Routine Monitoring: Security Events and Firewall Log Check	D-6
D.5 Routine Monitoring: Computer Assets.....	D-7
D.6 Routine Monitoring: Network Data Flow	D-10
D.7 Routine Monitoring: Synchronicity Check.....	D-11
ENCLOSURE E: FULLY MISSION-CAPABLE (FMC) BASELINE.....	E-1
E.1 FMC Baseline Introduction.....	E-1
E.2 FMC Baseline Overview.....	E-1
E.3 FMC Baseline Procedures	E-1
E.4 FMC Baseline Instructions	E-2
E.5 FMC Baseline Creation: ICS Enclave Entry Points.....	E-3
E.6 FMC Baseline Creation: Servers/Workstations	E-6
E.7 FMC Baseline Creation: Network Traffic	E-11
ENCLOSURE F: JUMP-KIT	F-1
F.1 Jump-Kit Introduction	F-1
F.2 Jump-Kit Contents.....	F-1
F.3 Jump-Kit Maintenance.....	F-2
F.4 Jump-Kit Rescue CD.....	F-2
ENCLOSURE G: DATA COLLECTION FOR FORENSICS.....	G-1
G.1 Data Collection for Forensics Introduction	G-1
G.2 Documentation of Data Collection.....	G-1
G.3 Data Collection Tools	G-1
G.4 Capturing Memory Data.....	G-2
G.5 Windows Registry Data	G-2

ENCLOSURE H: MITIGATION ISOLATION AND PROTECTION	H-1
H.1 Isolation and Protection Introduction.....	H-1
H.2 Isolation and Protection Overview.....	H-1
H.3 Creating a Segmentation Strategy	H-2
H.4 Suggested Segmentation Areas	H-2
ENCLOSURE I: CYBER SEVERITY LEVELS.....	I-1
I.1 Cyber Severity Levels Introduction	I-1
I.2 Cyber Severity Levels Overview.....	I-1
I.3 Incident Severity Levels.....	I-1
I.4 Precedence and Category Levels.....	I-2
I.5 Malicious Actions Table.....	I-2
APPENDIX A: SUPPORTING MATERIALS.....	AA-1
AA.1 System Characterization Guidelines	AA-1
AA.2 Characterizing ICS (Establishing the Baseline).....	AA-1
AA.3 Collaborating with Network Managers and Establishing Restoration Point.....	AA-2
AA.4 Routers and Switches.....	AA-2
AA.5 Servers and Workstations.....	AA-2
AA.6 Network Architecture	AA-3
AA.7 Data Flow Diagrams	AA-3
AA.8 Authorized User List	AA-3
AA.9 Notifications	AA-3
AA.10 Training Requirements and Recommendations	AA-4
AA.11 ICS Position Responsibilities	AA-6
AA.12 Cyber Incident Analysis Tools.....	AA-10
AA.13 Cyber Incident Documentation.....	AA-10
AA.14 Cyber Incident Reporting	AA-10
AA.15 Integration with CJCSM 6510.01B Requirements	AA-10
APPENDIX B: ACRONYMS AND ABBREVIATIONS	AB-1
APPENDIX C: DEFINITIONS	AC-1
APPENDIX D: REFERENCES.....	AD-1
APPENDIX E: TECHNICAL SUPPLEMENT	AE-1

This page intentionally left blank.

CHAPTER 1: ACI TTP OVERVIEW

1. Purpose

The purpose of this ACI TTP is to provide procedures that will enable IT and ICS managers to *Detect* nation-state-level cyber attacks; *Mitigate* the effects of those attacks; and *Recover* their networks following attacks.

2. Scope

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.

SCADA systems are generally used to control dispersed assets using centralized data acquisition and supervisory control. DCS are generally used to control production systems within a local area such as a factory using supervisory and regulatory control. PLCs are generally used for discrete control for specific applications and generally provide regulatory control. These control systems are vital to the operation of the DoD's critical infrastructures that are often highly interconnected and mutually dependent systems.

The ACI TTP is designed for ICS networks and the IT components that are used in them. While the ACI TTP does not include procedures regarding the Non-classified Internet Protocol Router Network (NIPRNet) and/or the corporate network, it does presume that both are hostile networks. ICS network staff should not rely on the cyber security infrastructure that these networks provide and should maintain a level of awareness regarding potential cyber attacks coming from these networks.

3. How to Use These TTP

This ACI TTP is divided into 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 E)

- a. **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.

- 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.

The primary goal of Mitigation Procedures (enclosure B) is to retain operations of the commander's functional priorities during an active cyber attack (e.g., electric, water, etc.). The TTP achieves this goal by segregating the attack, often requiring a degradation of the network's functionality. This could include the segregation of some portion of the ICS while the remaining portions operate under local control (meaning a loss of centralized control). There are two methodologies to consider when performing Mitigation: isolation and protection. Enclosure H: Mitigation Isolation and Protection provides best practices to consider when implementing these Mitigation methods.

Finally, ICS and IT personnel will use the Recovery Procedures (enclosure C) to restore the ICS to a "fully mission-capable" (FMC) state. The Recovery TTP is complete when the ICS is fully integrated and tested. The Recovery TTP presumes close coordination with the command's Information Systems Security Manager (ISSM) and the relevant DoD incident responders and ensures that detailed reporting (e.g. JIMS) is updated with current status.

- c. **Baselining and Routine Monitoring of the Network.** Before the ACI TTP is 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.

After determining the FMC baseline, routine monitoring of the network should be performed. Refer to Enclosure D: Suggested Routine Monitoring Procedures.

- d. **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).

4. 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.

Note: This TTP's guidance on incident handling, reporting, and unique response for DoD control systems is intended to be supplemental to the guidance found in Chairman of Joint Chiefs of Staff Manual (CJCSM) 6510.01B, Cyber Incident Handling Program, dated July 10, 2012. More information regarding CJCSM 6510.01B is located in appendix A, section AA.15 of the ACI TTP.

- 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.
- 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.
- 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.

Figure 1-1 depicts the high-level overview of the ACI TTP beginning with Detection, progressing to Mitigation, and then further progressing to Recovery.

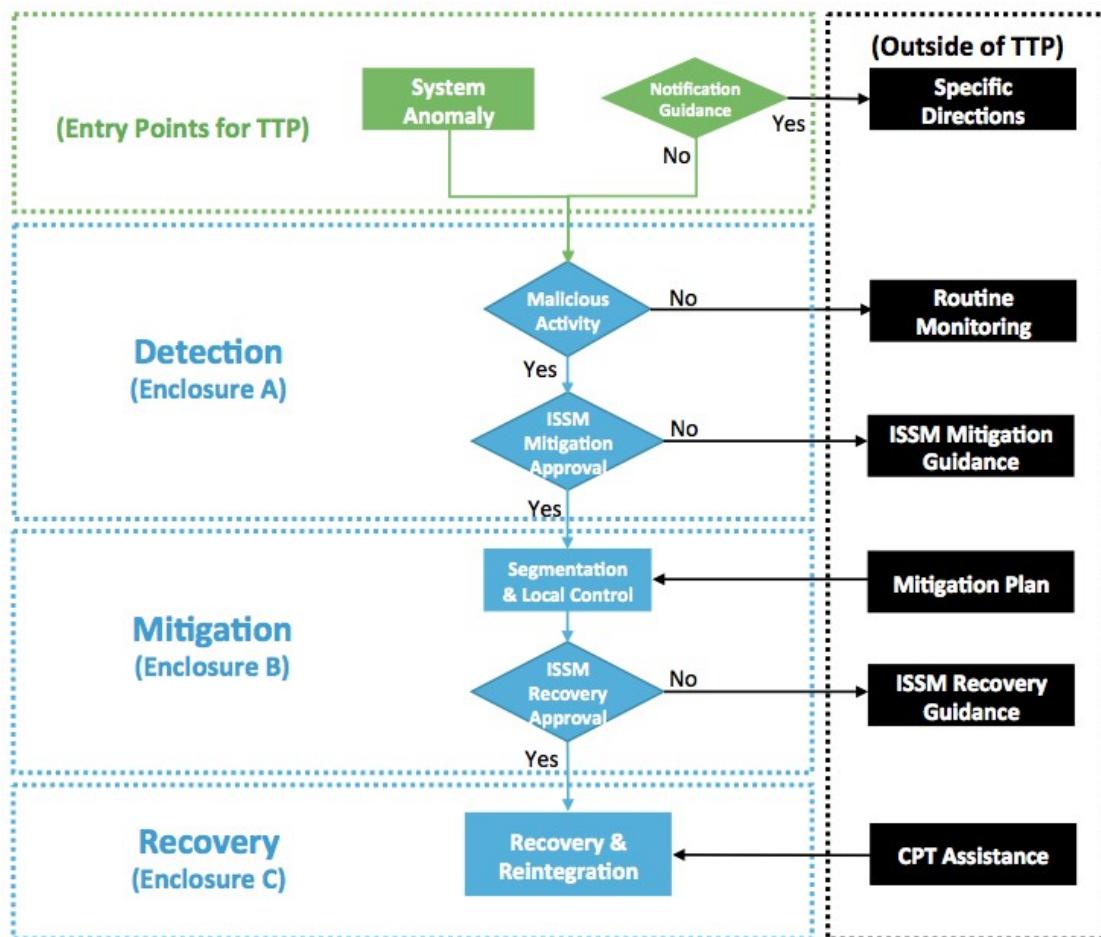


Figure 1-1: Detection, Mitigation, and Recovery Overview

5. 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.

6. CIA Triad

One significant difference between IT and ICS can be understood through the confidentiality, integrity, and availability (CIA) triad. This triad is a model, designed to guide policies for information security within an organization. While each part of the triad is important, in IT the emphasis is on confidentiality and integrity. In the ICS environment, availability is the most important part of the triad. Blocked or delayed information flows can disrupt ICS operation. As a result, it is important to consider the impact common IT tools could have on an ICS network. For example, using host-based security systems, network mapping tools, and vulnerability scanners on an ICS network could shut down the network and disrupt operations. This is important to remember when baselining, testing, or monitoring ICS networks.



7. 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.

Table 1-1 is an example Operational Security Log. A log should be designed to reflect and accommodate your environment and organizational requirements.

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

Table 1-1: Operational Security Log

This page intentionally left blank.

CHAPTER 2: ACI TTP DETECTION CONCEPTS

1. 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

2. Detection Overview

Detection through user observation is an “after-the-fact” activity. Relying on observable system behaviors carries a degree of risk. After-the-fact means an intrusion has occurred and the attack is in the process of delivering its payload. This payload could be either something that is focused on destruction or exfiltration. The result of relying on this level of detection could mean damage to the physical system or equipment, loss of critical data, alterations in software configuration that could produce undesirable effects to field devices, or the injection of malware that could deny the operations of the system or alter its behavior.

Given the numerous possible effects, the Detection Procedures (enclosure A) are designed to detect a malicious cyber event as early as possible. The basic actions involved with detection are routine monitoring, inspection, and transition to the Mitigation Procedures (enclosure B). Embedded within each of these phases are investigation and decision points.

Routine monitoring is one of two potential entry points to the detection phase. ICS operators execute daily monitoring routines. These consist of performing periodic equipment checks, tuning loops, checking set points, etc. The ACI TTP adapts the concept of routine maintenance monitoring to the cyber security world by including suggested routine monitoring activities. Refer to enclosure D. This enclosure provides monitoring activity best practices involving routine checks that can be integrated into normal ICS operations and monitoring schedules.

When an anomalous event is observed during Routine Monitoring, or an official notification of a cyber attack is received; the IT or ICS operator should immediately enter the Detect portion of the

TTP (enclosure A). The first step in the Detection portion of the TTP is to consult the *Event Diagnostics Table* (enclosure A, section A.1, table A.1.1).

3. Detection Process

ACI TTP Entry Points

1. Anomalies found during Routine Monitoring
2. Command directives, Warning Order (WARNORDS), Tasking Order (TASKORDS), IAVA Messages, Alerts or Bulletins, ICS-CERT Notices or other official notifications

In the absence of a WARNORD/TASKORD or other notification, and in the absence of anomalous symptoms, the ACI TTP assumes operators are conducting Routine Monitoring Procedures.

- a. If during the process of executing Routine Monitoring a cyber notification is issued, operators should execute the *Official Notifications* procedure listed in the *Event Diagnostics Table* (section A.1). This table has a column containing types of system or network behaviors that were observed, associated with an event, and page numbers directing to related diagnostic procedures.
- b. If anomalous symptoms are observed, operators should investigate to determine if these are hardware/software malfunctions or administrative issues. If the anomaly cannot be explained or corrected through normal troubleshooting activities, operators should check for a cyber event using the *Event Diagnostics Table* (section A.1). Operators should locate the observed symptoms and execute the Detection steps associated with the observed events located in enclosure A. Once located, the operators should continue to the specific diagnostic procedure in the *Event Diagnostic Procedures* (section A.2).
- c. Each *Event Diagnostic Procedure* identifies one or more *Integrity Checks* (enclosure A, section A.3, *Integrity Checks*, table A.3.1). *Integrity Checks* are to be completed in order of suggested priority. However, the order of *Integrity Checks* and the selection of *Integrity Checks* should be based on the operators' knowledge, experience, training, local policy and procedures. The series of events that invoke the ACI TTP process factor into the integrity check selection process. After each integrity check is completed, return to the diagnostic procedure.
- d. If at any time a Severity Level of *High* is identified, exit the Detect phase and request a transition from Detection to Mitigation from the ISSM.
- e. Routine Monitoring involves regular maintenance procedures conducted routinely by operators of ICS, infused with cyber monitoring activities. Cyber Routine Monitoring provides ICS operators with a set of activities that can be modified and adapted to full compliance with the DoDI 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT)*, dated March 12, 2014 (Appendix D: References).

Figure 2-1 depicts the flow within the Detect portion of the ACI TTP.

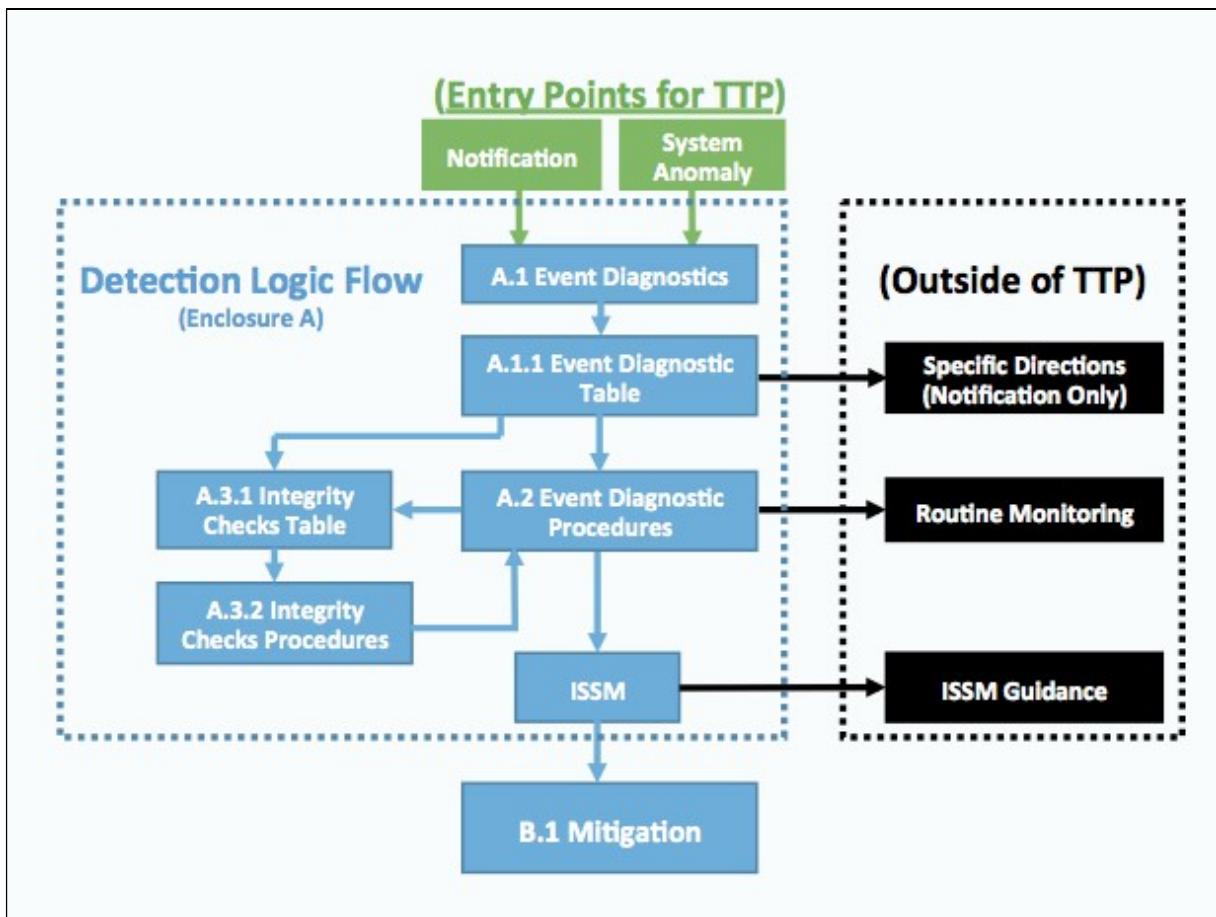


Figure 2-1: Flow Chart of Detection

This page intentionally left blank.

CHAPTER 3: ACI TTP MITIGATION CONCEPTS

1. Mitigation Introduction

- a. Definition. The actions taken that allow the ICS 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) Reporting and appropriate notifications
 - (3) Security log
- d. Mitigation Scope
 - (1) The ACI TTP cannot determine the scope of Mitigation required or necessary for every situation because ICS and IT systems differ greatly across the DoD. There are outside factors that may inform the scope of the Mitigation. It is the responsibility of the ISSM and outside resources to determine what Mitigation scope is appropriate for an incident. The operator and ISSM should have criteria in place for their specific system prior to an event, because this will assist them in determining the best course of action to take if an incident requires Mitigation. Enclosure H: *Mitigation Isolation and Protection* can assist in creating a Mitigation Plan.
 - (2) Organizations should consider the following factors to assist in determining the scope of Mitigation (in addition to any factors identified through the organization's risk management process):
 - a. Severity Level of the incident
 - b. Criticality of the system affected
 - c. Layer the incident resides on or affects
 - d. Whether the incident affects end-state processes
 - e. Operations that the system is controlling
 - f. Outside influences and events
 - (3) Once the scope of Mitigation has been determined and approved by the ISSM, the operators will utilize the instructions in the Mitigation Procedures (enclosure B) to assist them in conducting the Mitigation step most appropriate for the incident and the system it is affecting.

2. Mitigation Overview

The purpose of the Mitigation phase is to isolate and prevent further malicious activity while enabling the network and its endpoint devices to continue to execute its mission, even if it is in a reduced capacity.

The Mitigation phase begins when the operator is directed to the Mitigation Procedures (enclosure B) from an event diagnostic procedure within the Detection phase. The intent of the Mitigation phase is to protect the information system and network by ensuring that a cyber incident does not further propagate into the ICS system, and to acquire and protect data for analysis while maintaining operations during an active attack. This is achieved through the use of Mitigation actions linked to potential attack vectors which can be utilized to Mitigate a number of attacks against the ICS/SCADA.

The Mitigation Procedures build upon the Detection actions taken in the previous section to provide the operator with a procedural route to execute during an incident.

3. Mitigation Process

- a. 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. This should be performed only after careful consideration has been given to this fact and with commander approval.

Chairman of Joint Chiefs of Staff Manual (CJCSM) 6510.01B, *Cyber Incident Handling Program*, dated July 10, 2012, (appendix A, section AA.15) provides Department of Defense cyber incident handling procedures for routine responses to cyber events and incidents, and also outlines reporting criteria. According to CJCSM 6510.01B, “The information system will not be shut down or disconnected from the information network prior to acquiring and preserving the data unless authorized by the Computer Network Defense Service Provider (CNDSP), AKA Cyber Security Service Provider (CSSP), or command authority.”

When possible, all data should be acquired and preserved for further analysis. This includes volatile data, persistent data, and environmental data. If the situation does not permit this collection of data due to mission-critical responsibilities, the command authority must approve that the data acquisition will not be completed. For additional information on forensic analysis, please refer to Enclosure G: Data Collection for Forensics.

- b. Cyber Incident Response. Organizations, entities, and/or teams (assembled and trained in advance) must be prepared 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 be tested, trained, or exercised in advance.

- c. Mitigation Course of Action (COA). Develop a plan that lists the specific mitigation steps to take and identify the personnel (by job description) who are responsible for taking those steps. Identify the personnel/role that will act as lead. 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.

Various questions arise when deciding whether to contain malicious or unauthorized activity. Answers to these questions may require discussions with IT and business process owners, as well as with the Commander and legal advisors. Such questions might include:

- (1) Is it appropriate to shut down or disconnect an information system?
- (2) Do local system administrators and operators have the authority to shut down or disconnect an information system?
- (3) When must an information system stay up and running?
- (4) Which information systems cannot be taken offline or disconnected?
- (5) Are there investigative or intelligence equities to consider?
- (6) What existing policies and regulations apply?
- (7) What policy needs to be amended or MOU needs to be authored (if any)?

Organizations should develop appropriate containment strategies for critical assets in advance of mitigation. By preparing in this way, the need for decision-making will not occur at the time of an incident.

- d. Jump-Kit Mitigation. Actions may at times require the use of the Jump-Kit discussed in Enclosure F: Jump-Kit. This Jump-Kit can be used for analysis and for taking local control of devices.
- e. Caveats for Mitigation. Do not physically reconnect any piece of equipment until you have verified that it is clean, configured properly, and performing correctly as detailed in Enclosure C: Recovery Procedures.

This page intentionally left blank.

CHAPTER 4: ACI TTP RECOVERY CONCEPTS

1. Recovery Introduction

- a. Description. Restoration and reintegration of the ICS to a FMC 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

2. Recovery Overview

CJCSM 6510.01B requires development of a COA for response to cyber incidents. The Recovery ACI TTP (enclosure C) is intended to be supplemental to the CJCSM 6510.01B COAs. More information regarding CJCSM 6510.01B is located in appendix A, section AA.15. Because of the wide variance in ICS/SCADA system design and applications, the Recovery Procedures (enclosure C) associated with the ACI TTP are not specific to a particular make or model of equipment but are general in terms of application.

The operator **must not** proceed with Recovery Procedures without proper reporting and 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, provide technical assistance, detect lateral movement and develop mitigation strategies to thwart future compromises. 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.

In the event of a crisis or national emergency, restoration of the systems affected by the attack may take precedence over efforts to preserve forensic evidence. Ensure that proper authorization is received in order to proceed in this manner.

A cyber incident is a reportable event per CJCSM 6510.01B. Operators should record all Recovery actions. These records will be used as part of post-cyber incident forensics investigation, and will aid in reducing the likelihood of a recurrence of the cyber incident.

3. 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 ICS system schematics, and the wiring and logic diagrams, and may require vendor assistance. Successful Recovery of the ICS system after the cyber incident will depend upon the technical knowledge and skills of the ICS 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 reimage affected devices with known good firmware and/or software. In support of CJCSM 6510.01B incident response actions, efforts should be made to save a copy of the infected firmware/software for forensic analysis purposes. Vendor assistance may be required in order to perform these tasks.
- 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 mission commanders. 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 command.
 - (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. Risk analysis decisions should be documented in the corresponding cyber incident report.

4. Sequences and Reintegration for Recovery

- a. **Mission Commander Priorities**. The procedure for sequencing recovered devices should be based upon priorities established by the commander or the ISSM. Critical mission requirements and system interdependencies will be factors to consider in sequencing the Recovery process. For example, if mission requirements demand that the critical server heating, ventilation, and air conditioning (HVAC) systems are to be returned to service first, interdependency dictates that the electric power system should be recovered first since the HVAC cannot operate without it.
- b. **Reintegration**. Once the sequencing process has been established, the reintegration process should follow systematic steps that Recover individual devices first. Prior to performing reintegration of affected components, consult with the ISSM and use the records created while performing these procedures to ensure that remnants of the cyber attack have been cleaned from every component affected. Once individual devices in a functional group have been tested, reintegrate the sub-system (functional equipment groups) and, finally, reintegrate the network layers. Always verify each device is free from malware and abnormal behavior prior to reconnecting it to adjacent devices.
- c. **Recovery**. Recovered networks should have stringent monitoring in place to ensure that all malware remnants from the cyber incident have been eliminated from the network. Coordination with the supported CSSP should be maintained so that they can assist with notification of JFHQ-DoDIN, and USCYBERCOM for additional network monitoring at a higher tier.

This page intentionally left blank.

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-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. Observe and alert when an asset or device communicates with other devices outside of the FMC data flow baseline.	A-12

A.1.1 Event Diagnostics Table - Continued

Section	Event	Description	Page
A.2.8	Unexpected Behavior: HMI, OPC, and Control Server	<p>Unexpected behavior of an HMI, OPC, or control server affecting controllers. Examples of unusual communications:</p> <ol style="list-style-type: none"> 1. HMI, OPC, and controllers not synchronized. 2. Unexpected changes to instructions, function calls, commands, or alarm thresholds being sent from HMI or OPC to controllers. 3. HMI or OPC not updating after operator made changes to instructions, commands, or alarm thresholds. 4. Expected changes to controllers are not appearing on controllers. 5. HMI, OPC, or control server reboots and unexpected changes to settings are sent to controller. 	A-13
Network Anomalies			
A.2.9	Loss of Communications	Network devices are no longer communicating with other devices, servers, or workstations.	A-14
A.2.10	Unusually High Network Traffic	ICS network traffic appears unusually busy, either between devices, or across the ICS boundary.	A-15
A.2.11	At Network Entry Points - Network Flow - Unusual Traffic	An unusual Internet protocol (IP) address or an unusual port, protocol, or service (from a known IP address) is attempting to communicate with the ICS.	A-16
A.2.12	IDS Exhibiting Unusual Behavior	Intrusion detection system (IDS) is degraded and is not issuing alerts or logs, keyboard locked, spontaneous reboot, anomalous display screen changes, or any anomalous symptom.	A-17
A.2.13	Firewall Log Indicates Anomalous Event Occurred	Anomalous events include: inbound or outbound traffic from unknown IP, inbound simple mail transfer protocol (SMTP) (email) from unknown IP, inbound or outbound ICS control protocol traffic, inbound or outbound Telnet, file transfer protocol (FTP), trivial file transfer protocol (TFTP), hypertext transfer protocol (HTTP), secure hypertext transfer protocol (HTTPS) to or from unknown IP, or anomalous firmware pushes or pulls.	A-18
A.2.14	Firewall Exhibiting Unusual Behavior	Firewall does not log or alert, keyboard is locked (host-based firewall), spontaneous firewall reboots, display screen changes for no reason (host-based firewall), or any unusual symptom (e.g. host-based firewall is turned off, is suspended, fails, or corresponding service won't start).	A-19
A.2.15	Abnormal Peripheral Device Communications	A peripheral device (such as a printer, fax machine, copier, repeaters, hubs, converters, etc.) is attempting to communicate with devices it normally does not communicate with, uses a services which is not typical, or is communicating abnormally, such as scanning other devices within a network.	A-20
A.2.16	IP Address Originating From Two or More MAC Addresses	Observe and alert if a single IP address is observed originating from two or more media access control (MAC) addresses. This may indicate that an attacker is spoofing an IP address.	A-21

A.1.1 Event Diagnostics Table - Continued			
Section	Event	Description	Page
Field Device Anomalies			
A.2.17	Abnormal Decrease in Control Process Traffic or Loss of Communications	The normal flow of control traffic appears slower, sluggish, or there is less traffic than normal (polling cycles not executing for example).	A-22
A.2.18	Unusual Field Device Activity Observed/ Reported	Any anomalous behavior coming from field devices could be hardware malfunctions or communication path malfunctions. However, once these have been ruled out, a cyber incident should be considered as the possible source of the problem.	A-23
A.2.19	Unexpected Changes to Ladder Logic/Code Configurations, Firmware, and Set Points	Changes to the controller logic within the field device could come from a process that has been altered, a new process that has been implemented, an old process that was removed, or a process that was hijacked.	A-24
A.2.20	HMI, OPC, or Control Server Sending False Information	If false information is sent to the control system, it could either be an error, or a malicious attempt to disguise unauthorized changes or an initiation of inappropriate actions by system operators.	A-25
A.2.21	Anomalous Safety Systems Modifications	Anomalous modifications to the safety system could come from an error in the system, accidental misconfiguration, or some other explained event. If the change to the safety system cannot be explained, the changes could be malicious with the intention of damaging the control system.	A-26
IDS Alerts			
A.2.22	Unexpected Patch Update (Not Announced By Vendors)	The IDS and/or regular system maintenance observed an irregular vendor patch coming from an external source, or unexpected source, to a device within the ICS.	A-27
A.2.23	Asset Communicating With an Undocumented, Unauthorized, or Unknown IP Address	Host, peripheral, field controller, or intelligent field device communicating with an undocumented, unauthorized, or unknown IP address. Data flow traffic, boundary traffic, or host connections reveal device is communicating with an unknown IP address.	A-28
A.2.24	Inbound ICS Protocol Traffic From Unknown or External IP Address	Inbound ICS protocol, such as Modbus, distributed network protocol (DNP3), or other ICS protocols from unknown or external IP address. A device other than the normal control server, OPC, or HMI (or other authorized devices) is sending field controller traffic to a field device.	A-29

A.1.1 Event Diagnostics Table - Continued			
Section	Event	Description	Page
A.2.25	Inbound or Outbound HTTP or HTTPS to or From Unknown or External IP Address	Traffic coming or going to an unknown device. For example, HTTP or HTTPS traffic in a network segment where these protocols should not be used.	A-30
A.2.26	Unexpected Connection to External or Unknown IPs	An ICS field controller is communicating with an unknown device or machine.	A-31
A.2.27	Unusual Lateral Connections (Connections in the Same Network Segment) Between ICS Assets	An ICS device or machine has expanded its communications to other devices or machines within the ICS.	A-32
A.2.28	All Other Alerts	IDS can alert on a wide variety of events. Some are false positives. Coordinate with the IDS team to refine signatures to reduce false positive alerting.	A-33

A.2. Event Diagnostic Procedures

A.2.1 Notifications	
Step	Procedures
Investigation	<p>1. DETERMINE if you have assets affected by the Notification:</p> <ol style="list-style-type: none"> OBTAIN FMC Baseline Topology. CROSS REFERENCE assets listed in the Notification with assets in the <i>FMC Baseline Topology</i>. If assets listed in the Notification cannot be found in the <i>FMC Topology</i>, and you have no knowledge of such assets being on your installation, then the notification does not pertain to your ICS.
No Action Required	<p>2. If assets in Notification are not in your ICS:</p> <ol style="list-style-type: none"> DOCUMENT the Severity Level as None (0) in the Security Log. RETURN to <i>Routine Monitoring</i>.
If Action Required	<p>3. If Notification pertains to your ICS, and the Notification includes specific procedures:</p> <ol style="list-style-type: none"> DOCUMENT in Security Log. EXIT the ACI TTP and EXECUTE the steps listed in Notification. <p>4. If the Notification pertains to your ICS but does not have specific procedures, or if it is undetermined whether the Notification pertains to your ICS:</p> <ol style="list-style-type: none"> DOCUMENT in Security Log. SEARCH your system for any indicators specifically identified by, or related to, the notification. If server/workstation anomalies are present, use the <i>Event Diagnostics Table</i> starting on page A-1 to IDENTIFY specific procedures capable of satisfying the notification. If server/workstation anomalies are NOT present, go directly to section A.3, <i>A.3.1 Integrity Checks Table</i> and locate the appropriate integrity checks for assets affected by the notification and execute the integrity checks. <p>Recommended Checks: Any Integrity Check may be applicable.</p> <p>5. Once you have completed all appropriate Integrity Checks, GO TO section A.2.29 Action Step.</p>
END OF NOTIFICATIONS	

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

- **Functional Area:** IT or ICS
- **Description:** Any computer based server, workstation, including SCADA equipment. Anomalous entries can include (but not limited to):
 1. Unauthorized user logging in
 2. Rapid and/or continuous log-ins/log-outs
 3. Users logging into accounts outside of normal working hours and for no apparent reason
 4. Numerous failed log-in attempts found in logs on administrator accounts or other user accounts
 5. User accounts attempting to escalate account privileges or access areas or assets not required by their jobs (see Appendix E, section EE.16)
 6. Detect unauthorized usage of administrative tools/utilities (see Appendix E, section EE.17)

Step	Procedures
Investigation	<ol style="list-style-type: none"> 1. DETERMINE if any of the following events occurred: <ol style="list-style-type: none"> a. Personnel changes were made. b. Systems administrator may be on leave or absent and duties have been delegated to another user. c. Other authorized user event occurred.
No Action Required	<ol style="list-style-type: none"> 2. If the unexpected use of the user account is authorized: <ol style="list-style-type: none"> a. DOCUMENT the Severity Level as None (0) in the Security Log. b. CONTINUE with the next diagnostic procedure. If all applicable procedures have been completed, RETURN to <i>Routine Monitoring</i>.
If Action Required	<ol style="list-style-type: none"> 3. If the unexpected use of the user account is not authorized: <ol style="list-style-type: none"> a. DOCUMENT in Security Log. b. GO TO Section A.3, A.3.1 <i>Integrity Checks Table</i>. (See recommended checks below.) LOCATE the Integrity Checks associated with asset you are investigating and EXECUTE the integrity checks. <p style="padding-left: 20px;">Recommended Checks:</p> <ul style="list-style-type: none"> A.3.2.3 Unauthorized User Account Activity A.3.2.2 Server/Workstation Log Review 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.2.3 Server/Workstation: Irregular Process Found	
Step	Procedures
Investigation	<p>1. DETERMINE if the new process belongs to an authorized installation:</p> <ol style="list-style-type: none"> New software was installed on to the system? Was maintenance performed on the system, and if the new process was installed during that maintenance? Is the new process a result of a patch update?
No Action Required	<p>2. If the new process belongs to an authorized installation:</p> <ol style="list-style-type: none"> DOCUMENT the Severity Level as None (0) in the Security Log. CONTINUE with the next diagnostic procedure. If all applicable procedures have been completed, RETURN to <i>Routine Monitoring</i>.
If Action Required	<p>3. If the new process does not belong to an authorized installation:</p> <ol style="list-style-type: none"> DOCUMENT in Security Log. GO TO Section A.3, A.3.1 <i>Integrity Checks Table</i>. (See recommended checks below.) LOCATE the integrity check associated with server or workstation you are investigating and EXECUTE the Integrity checks. <p>Recommended Checks:</p> <ul style="list-style-type: none"> 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 A.3.2.17 Server/Workstation Additional Checks <p>4. Once you have completed all appropriate Integrity Checks, GO TO section A.2.29 Action Step.</p>

A.2.4 Server/Workstation: Suspicious Software/Configurations	
Step	Procedures
Investigation	<p>1. DETERMINE if the Detection is from anti-virus software installed on a server or workstation, or from anomalous behavior consistent with symptoms of malicious code.</p>
No Action Required	<p>2. If the software perceived to be malicious is determined to not be malicious:</p> <ul style="list-style-type: none"> a. DOCUMENT the Severity Level as None (0) in the Security Log. b. CONTINUE with the next diagnostic procedure. If all applicable procedures have been completed, RETURN to <i>Routine Monitoring</i>.
If Action Required	<p>3. If the malware was Detected by antivirus software:</p> <ul style="list-style-type: none"> a. From the virus Detection software SELECT option to eradicate malware from the system. If the virus checking software is not able to completely remove the malware it may be necessary to research the malware to determine effective removal procedures. b. DOCUMENT results in the Security Log. <p>4. If the malware was not Detected by a virus checking software, or the device does not have a virus checking software package installed:</p> <ul style="list-style-type: none"> a. Run a cryptographic hash of the file using one of following utilities: <ul style="list-style-type: none"> • Certutil (see Appendix E, section EE.2) • Sigcheck (see Appendix E, section EE.15) b. DOCUMENT in Security Log. c. RETRIEVE virus removal compact disk (CD) from emergency Jump-Kit. d. UPDATE virus removal CD with the latest virus signatures using the Jump-Kit laptop (clean machine). e. Using the Jump-Kit instructions for virus removal, EXECUTE virus removal procedures. If malicious files are not removed or found, run the additional anti-malware utilities from the jump-kit CD. f. Upon completion, RUN a full virus scan of the machine. g. GO TO Section A.3, A.3.1 <i>Integrity Checks Table</i>. (See recommended checks below.) LOCATE integrity check for the server or workstation you are working, and EXECUTE the integrity checks. <p>Recommended Checks:</p> <ul style="list-style-type: none"> A.3.2.2 Server/Workstation Log Review A.3.2.1 Server/Workstation Process Check A.3.2.4 Server/Workstation Communications Check A.3.2.13 Server/Workstation Rootkit Check A.3.2.17 Server/Workstation Additional Checks <p>5. Once you have completed all appropriate Integrity Checks, GO TO section</p>

A.2.4 Server/Workstation: Suspicious Software/Configurations	
	A.2.29 Action Step.

A.2.5 Server/Workstation: Irregular Audit Log Entry (Or Missing Audit Log)	
Step	Procedures
Investigation	<p>1. DETERMINE if irregular audit log entry/condition was caused by an authorized event:</p> <ol style="list-style-type: none"> Was maintenance conducted on the machine, and the log was altered? Did the machine malfunction? Was the machine restored from a backup? Did the machine lose connectivity?
No Action Required	<p>2. If the irregular audit log entry or condition was caused by an authorized event:</p> <ol style="list-style-type: none"> DOCUMENT the Severity Level as None (0) in the Security Log. CONTINUE with the next diagnostic procedure. If all applicable procedures have been completed, RETURN to <i>Routine Monitoring</i>.
If Action Required	<p>3. If the irregular audit log entry or condition was not created by an authorized event:</p> <ol style="list-style-type: none"> DOCUMENT in Security Log GO TO Section A.3, A.3.1 <i>Integrity Checks Table</i>. (See recommended checks below.) LOCATE the integrity check for the server or workstation you are investigating, and EXECUTE the integrity checks. <p>Recommended Checks:</p> <ul style="list-style-type: none"> A.3.2.2 Server/Workstation Log Review A.3.2.1 Server/Workstation Process Check A.3.2.6 Server/Workstation Registry Check (MS Windows Only) A.3.2.13 Server/Workstation Rootkit Check A.3.2.17 Server/Workstation Additional Checks <p>4. Once you have completed all appropriate Integrity Checks, GO TO section A.2.29 Action Step.</p>

A.2.6 Server/Workstation: Unusual System Behavior

- **Functional Area:** IT or ICS
- **Description:** Any computer based server, workstation, including SCADA equipment:
 1. Spontaneous reboots
 2. Spontaneous screen saver change
 3. Unusually slow performance
 4. Unusually active CPU
 5. CPU cycles up and cycles down for no apparent reason
 6. Intermittent loss of mouse or keyboard
 7. Configuration files changed without user or system administrator action in operating system
 8. Configuration changes to software made without user or system administrator action
 9. Programs running on computer (remote login)
 10. System unresponsive
 11. Network Card is in promiscuous mode (see Appendix E, section EE.12)
 12. Review unexpected files possibly resulting from malware. Review **new** and/or **unexpected** files, including the following types (Note: these file extensions are also used for legitimate files):
 - a. unexpected log files (e.g. *.log)
 - b. unexpected scripting files (e.g. *.py, *.vbs, *.js, *.bat, *.ps1, *.pl, *.cmd)
 - c. unexpected executable files (e.g. *.exe, *.bin.*.com)
 - d. unexpected Windows registry files (e.g. *.reg)
 13. Review unexpected network capture files possibly resulting from malicious monitoring:
 - a. unexpected *.pcap (Wireshark/Tshark/etc.)
 - b. unexpected *.etl (Microsoft Net Trace)
 14. Detect malicious “Wiper”-type malware overwrite of ICS file types (review both local and mapped network drives). Also review for overwrite of local Windows system files. (see Appendix E, section EE.13)

Note: By the time wiping activity occurs it may be too late to review (system may be unresponsive).
 15. Detect unexpected encrypted or high entropy files (See Appendix E, section EE.14)

Step	Procedures
Investigation	<ol style="list-style-type: none"> 1. Determine if the system is responsive: <ol style="list-style-type: none"> a. If unresponsive, GO TO A.3.2.5 Server/Workstation Unresponsive Check. b. If responsive: <ol style="list-style-type: none"> (1) If the system can be accessed directly or with tools, continue to Step 2. (2) If the system cannot be accessed directly or with tools, IDENTIFY any other server or workstation that can be accessed and may also have unusual system behavior, continue to Step 2 and investigate those systems. If this is the only server or workstation that has unusual system behavior: <ol style="list-style-type: none"> 1 DISCONNECT the computer from network. 2 DOCUMENT the Severity Level as None (0). 3 FOLLOW normal troubleshooting and replacement procedures.

A.2.6 Server/Workstation: Unusual System Behavior	
	<p>4 RETURN to <i>Routine Monitoring</i>.</p> <p>2. DETERMINE if maintenance changes were made to the machine, thus causing abnormal behaviors (authorized upgrades, patch installations, configuration changes, etc.).</p> <ul style="list-style-type: none"> a. If maintenance changes were made, work with systems administrator to RESOLVE maintenance anomalies. b. If maintenance changes were not made, TROUBLESHOOT for hardware or software failures.
No Action Required	<p>3. If the unusual behavior was caused by a regular maintenance change or a hardware and/or software failure:</p> <ul style="list-style-type: none"> a. RESOLVE problems through normal repair processes. b. DOCUMENT the Severity Level as None (0) in the Security Log. c. CONTINUE with the next diagnostic procedure. If all applicable procedures have been completed, RETURN to <i>Routine Monitoring</i>.
If Action Required	<p>4. If the unusual behavior was not caused by a maintenance change, hardware or software failure:</p> <ul style="list-style-type: none"> a. DOCUMENT in Security Log. b. GO TO Section A.3, A.3.1 <i>Integrity Checks Table</i>. (See recommended checks below.) LOCATE the Integrity Check associated with the server or workstation you are investigating, and EXECUTE the integrity checks. <p>Recommended Checks:</p> <ul style="list-style-type: none"> A.3.2.2 Server/Workstation Log Review A.3.2.1 Server/Workstation Process Check A.3.2.6 Server/Workstation Registry Check (MS Windows Only) A.3.2.4 Server/Workstation Communications Check A.3.2.13 Server/Workstation Rootkit Check A.3.2.17 Server/Workstation Additional Checks <p>5. Once you have completed all appropriate Integrity Checks, GO TO section A.2.29 Action Step.</p>

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

- **Functional Area:** IT or ICS
- **Description:** Servers, workstations, 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. Observe and alert when an asset or device communicates with other devices outside of the FMC data flow baseline.
- Consider implementing IDS signatures (If IDS is available) to detect port scanning of common ICS ports (or tailor to the ports used within the environment). Malware may execute port scans in order to enumerate PIT/ICS devices on the local network and/or enumerate peer hosts to target for future lateral movement (**also see Check A.2.27**)

Here is an example list of ports to watch for using IDS port scan rules. You will need to tune these IDS rule(s) to trigger above the volume/patterns of authorized ICS traffic on your network.

BACnet/IP	UDP 47808
DNP3	TCP/UDP 20000
EtherCAT	UDP 34980
EtherNet/IP/CIP	TCP/UDP 44818, TCP/UDP 2222
FL-net	UDP 55000-55003
Foundation Fieldbus	TCP/UDP 1089-1091
IEC 61850	TCP 102
Modbus	TCP 502
OPC	TCP 4840 (and possibly also for 80, 443, however this may cause false positives)
PROFINET	TCP/UDP 34962-34964

- Also implement IDS signatures to detect port scanning of Enterprise admin ports and Windows ports

ssh	22
telnet	23
smb	139 and 445

Step	Procedures
Investigation	<ol style="list-style-type: none"> 1. DETERMINE if the new communications pattern is an authorized activity: <ol style="list-style-type: none"> a. Was the device reconfigured? b. Was a new network asset installed? c. Did any other authorized change happen on the network that could have caused this issue? 2. TROUBLESHOOT for hardware or software problems.
No Action Required	<ol style="list-style-type: none"> 3. If the new communication pattern was authorized, or the issue is related to software or hardware problems: <ol style="list-style-type: none"> a. DOCUMENT the Severity Level as None (0) in the Security Log. b. CONTINUE with the next diagnostic procedure. If all applicable procedures have been completed, RETURN to <i>Routine Monitoring</i>.
If Action	<ol style="list-style-type: none"> 4. If scanning activity is not related to an authorized event: <ol style="list-style-type: none"> a. DOCUMENT in Security Log.

Required	<p>b. GO TO Section A.3, A.3.1 <i>Integrity Checks Table</i>. (See recommended checks below.) LOCATE asset type that was conducting the scans and EXECUTE integrity checks.</p> <p>Recommended Checks:</p> <ul style="list-style-type: none">A.3.2.4 Server/Workstation Communications CheckA.3.2.2 Server/Workstation Log ReviewA.3.2.1 Server/Workstation Process CheckA.3.2.6 Server/Workstation Registry Check (MS Windows Only)A.3.2.13 Server/Workstation Rootkit CheckA.3.2.17 Server/Workstation Additional Checks <p>5. Once you have completed all appropriate Integrity Checks, GO TO section A.2.29 Action Step.</p>
----------	---

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

- **Functional Area:** IT or ICS
- **Description:** Unexpected behavior of an HMI, OPC, or control server affecting controllers.
Examples of unusual communications (but not limited to):
 1. HMI/OPC and controllers not synchronized
 2. Unexpected changes to instructions, function calls, commands or alarm thresholds being sent from HMI, OPC, or control server to controllers without operator action
 3. HMI, OPC, or control server not updating after operator made changes to instructions, commands, or alarm thresholds
 4. Field operators reporting that expected changes to controllers are not appearing on controllers
 5. HMI, OPC, or control server reboots and unexpected changes to settings are sent to controller
- Consider implementing IDS signatures (If IDS is available) to detect:
 1. Unexpected ICS protocol traffic with infinite (cycling or looped) commands (on/off, or iterating over a range)
 2. Unexpected/invalid ICS commands sent to controllers
 3. Unusual/invalid packets sent to controllers

Step	Procedures
Investigation	<ol style="list-style-type: none"> 1. DETERMINE if the anomalous system's behavior was due to a hardware/software failure or if there is a network malfunction.
No Action Required	<ol style="list-style-type: none"> 2. If the anomaly was due to a hardware/software or network failure: <ol style="list-style-type: none"> a. DOCUMENT the Severity Level as None (0) in the Security Log. b. CONTINUE with the next diagnostic procedure. If all applicable procedures have been completed, RETURN to <i>Routine Monitoring</i>.
If Action Required	<ol style="list-style-type: none"> 3. If the anomaly cannot be explained by a normal malfunction: <ol style="list-style-type: none"> a. DOCUMENT in Security Log. b. CHECK other assets that communicate with field controllers for a similar anomaly. <ol style="list-style-type: none"> (1) If similar anomalies are found on other assets, DOCUMENT in Security Log. (2) LOCATE asset types in Section A.3, A.3.1 <i>Integrity Checks Table</i>. (See recommended checks below.) EXECUTE the integrity checks. <p style="text-align: center;">Recommended Checks:</p> <ul style="list-style-type: none"> A.3.2.2 Server/Workstation Log Review A.3.2.1 Server/Workstation Process Check A.3.2.6 Server/Workstation Registry Check (MS Windows Only) A.3.2.4 Server/Workstation Communications Check A.3.2.13 Server/Workstation Rootkit Check

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

A.3.2.17 Server/Workstation Additional Checks

4. Once you have completed all appropriate Integrity Checks, **GO TO** section
A.2.29 Action Step.

END OF SERVER AND WORKSTATION ANOMALIES

A.2.9 Network Anomalies: Loss of Communications

- **Functional Area:** IT or ICS
- **Description:** A network device, server, workstation, peripheral, or control device has lost communications with the network

Step	Procedures
Investigation	<ol style="list-style-type: none"> 1. OBTAIN FMC Baseline Topology. 2. LOCATE device or asset that is no longer communicating. 3. DETERMINE if the asset was reconfigured or replaced and if the change was intentional and authorized. 4. DETERMINE if there is an obvious hardware, cable, or software failure.
No Action Required	<ol style="list-style-type: none"> 5. If the asset loss of communications is identified and the source is not malicious: <ol style="list-style-type: none"> a. DOCUMENT the Severity Level as None (0) in the Security Log. b. CONTINUE with the next diagnostic procedure. If all applicable procedures have been completed, RETURN to <i>Routine Monitoring</i>.
If Action Required	<ol style="list-style-type: none"> 6. If the loss of communications is not authorized or from a known communications problem: <ol style="list-style-type: none"> a. DOCUMENT in the Security Log. b. GO TO Section A.3, A.3.1 <i>Integrity Checks Table</i>. (See recommended checks below.) EXECUTE the integrity check associated with the device (example: printer, fax, modem, repeater, converters, etc.). <p style="margin-left: 20px;">Recommended Checks:</p> <ul style="list-style-type: none"> A.3.2.8 Validate Data Flow (Network Traffic) A.3.2.4 Server/Workstation Communications Check A.3.2.7 Switch/Router Integrity Check A.3.2.12 Other Network Device Integrity Check A.3.2.2 Server/Workstation Log Review A.3.2.1 Server/Workstation Process Check A.3.2.9 Controller Integrity Check 7. Once you have completed all appropriate Integrity Checks, GO TO section A.2.29 Action Step.

A.2.10 Network Anomalies: Unusually High Network Traffic

- **Functional Area:** IT or ICS
- **Description:** ICS network traffic appears unusually busy, either between devices, or across the ICS boundary
 1. Variances can occur during working hours when a variety of users log on to the system. However, these variances should not be highly noticeable.
 2. Unusually high network traffic, particularly when coupled with other anomalous behavior (such as the HMI or engineering workstation appearing unusually busy without user intervention), should be investigated.

Step	Procedures
Investigation	<p>1. Using your organization's normal network monitoring procedures, DETERMINE if:</p> <ol style="list-style-type: none"> a. Authorized and additional batch processes are executing. b. Processes involved with shift changes are executing. c. Full virus or network scans are executing. d. Other authorized events are causing excessive network traffic on the ICS. e. Identify unexpected network Flow volume when compared to baseline traffic recorded in table E-4: ICS Data Flow. If applicable, create anomaly detection signature in IDS or use NetFlow to assist with detection of differences.
No Action Required	<p>2. If the excess network traffic is authorized:</p> <ol style="list-style-type: none"> a. DETERMINE whether the baseline should be updated and DOCUMENT the Severity Level as None (0) in the Security Log. b. CONTINUE with the next diagnostic procedure. If all applicable procedures have been completed, RETURN to <i>Routine Monitoring</i>.
If Action Required	<p>3. If excessive network traffic is not authorized:</p> <ol style="list-style-type: none"> a. DOCUMENT in Security Log. b. GO TO Section A.3, A.3.1 <i>Integrity Checks Table</i>. (See recommended checks below.) LOCATE the Integrity Check associated with the network traffic. EXECUTE the integrity checks. <p>Recommended Checks:</p> <ul style="list-style-type: none"> A.3.2.8 Validate Data Flow (Network Traffic) A.3.2.4 Server/Workstation Communications Check A.3.2.11 Firewall Log Review <p>4. Once you have completed all appropriate Integrity Checks, GO TO section A.2.29 Action Step.</p>

A.2.11 Network Anomalies: At Network Entry Points - Network Flow - Unusual Traffic

- **Functional Area:** IT or ICS
- **Description:** An unusual IP address or an unusual port, protocol or service (from a known IP address) is attempting to communicate with the ICS

Step	Procedures
Investigation	<ol style="list-style-type: none"> 1. RETRIEVE ICS topology diagram and <i>Entry Point Traffic</i> table from the baseline documentation. 2. COMPARE observed network traffic to the baseline network traffic: <ol style="list-style-type: none"> a. Identify unexpected traffic parameters (IPs, Ports, Protocols, and Services) when compared to baseline traffic recorded in table E-4: ICS Data Flow. If applicable, create anomaly detection signature in IDS or use NetFlow to assist with detection of differences. Also see the following Checks: A.2.23, A.2.24, A.2.25, and A2.26. b. From a command line, run the “route print” command and look for any unexplained IPv6 entries (also ensure that IPv4 entries match baseline) c. DOCUMENT any differences. d. If differences are found, DETERMINE if the network traffic is authorized.
No Action Required	<ol style="list-style-type: none"> 3. If the network traffic is authorized: <ol style="list-style-type: none"> a. For any unexpected, but authorized activity, determine whether the baseline should be updated. b. DOCUMENT the Severity Level as None (0) in the Security Log. c. CONTINUE with the next diagnostic procedure. If all applicable procedures have been completed, RETURN to <i>Routine Monitoring</i>.
If Action Required	<ol style="list-style-type: none"> 4. If the network traffic is unauthorized: <ol style="list-style-type: none"> a. DOCUMENT in Security Log. b. OBTAIN the <i>FMC Baseline Topology</i>. c. LOCATE affected assets (destination IP(s) for anomalous traffic). d. GO TO Section A.3, A.3.1 <i>Integrity Checks Table</i>. (See recommended checks below.) LOCATE the affected asset(s) on the table (example: workstation, HMI, PLC, etc.), and EXECUTE integrity checks. <p style="text-align: center;">Recommended Checks:</p> <ul style="list-style-type: none"> A.3.2.2 Server/Workstation Log Review A.3.2.6 Server/Workstation Registry Check (MS Windows Only) A.3.2.7 Switch/Router Integrity Check A.3.2.10 Firewall Integrity Check A.3.2.11 Firewall Log Review A.3.2.12 Other Network Device Integrity Check A.3.2.14 IDS Integrity Check A.3.2.16 Peripherals Integrity Check

A.2.11 Network Anomalies: At Network Entry Points - Network Flow - Unusual Traffic

A.3.2.17 Server/Workstation Additional Checks

A.3.2.9 Controller Integrity Check

A.3.2.1 Server/Workstation Process Check

5. Once you have completed all appropriate Integrity Checks, **GO TO** section

A.2.29 Action Step.

A.2.12 Network Anomalies: IDS Exhibiting Unusual Behavior

- **Functional Area:** IT or ICS
- **Description:** IDS exhibiting unusual behavior:
 1. IDS not issuing alerts
 2. Keyboard locked
 3. Spontaneous reboot
 4. Anomalous display screen changes
 5. Any anomalous symptom

Step	Procedures
Investigation	<ol style="list-style-type: none"> 1. PERFORM routine trouble-shooting to rule out: <ol style="list-style-type: none"> a. Hardware malfunction. b. Software malfunction. c. Network communications malfunction. d. User error.
No Action Required	<ol style="list-style-type: none"> 2. If the problem was a hardware, software, or network communications malfunction: <ol style="list-style-type: none"> a. DOCUMENT the Severity Level as None (0) in the Security Log. b. CONTINUE with the next diagnostic procedure. If all applicable procedures have been completed, RETURN to <i>Routine Monitoring</i>.
If Action Required	<ol style="list-style-type: none"> 3. If the unusual behavior is not a hardware, software, or network malfunction: <ol style="list-style-type: none"> a. DOCUMENT in Security Log. b. GO TO Section A.3, A.3.1 <i>Integrity Checks Table</i>. (See recommended checks below.) LOCATE the integrity check associated with the affected devices. EXECUTE the integrity checks. <p style="margin-left: 20px;">Recommended Checks:</p> <ul style="list-style-type: none"> A.3.2.14 IDS Integrity Check A.3.2.2 Server/Workstation Log Review A.3.2.6 Server/Workstation Registry Check (MS Windows Only) A.3.2.1 Server/Workstation Process Check A.3.2.4 Server/Workstation Communications Check A.3.2.5 Server/Workstation Unresponsive Check <p>4. Once you have completed all appropriate Integrity Checks, GO TO section A.2.29 Action Step.</p>

A.2.13 Network Anomalies: Firewall Log Indicates Anomalous Event Occurred

- **Functional Area:** IT or ICS
- **Description:** Firewall
Anomalous events include (not limited to):
 1. Inbound or outbound traffic between ICS network and any other network, including the Internet
 2. Inbound SMTP (email) from unknown IP
 3. Inbound or outbound ICS control protocol traffic (e.g., Modbus, DNP3, etc.)
 4. Inbound or outbound Telnet, FTP, TFTP, HTTP, HTTPS to or from unknown IP
 5. Anomalous firmware pushes or pulls
 6. Detect queries to multiple sites via IP not DNS.
 7. Detect queries to multiple sites for same file (however, edge cache/cloud may cause false positives for patches).

Step	Procedures
Investigation	<ol style="list-style-type: none"> 1. OBTAİN FMC Baseline Documentation. 2. LOCATE asset(s) involved with the Security Log entry. 3. DETERMINE if the event on those assets is an authorized event.
No Action Required	<ol style="list-style-type: none"> 4. If the event was authorized: <ol style="list-style-type: none"> a. DOCUMENT the Severity Level as None (0) in the Security Log. MARK entry as a <i>Notice to Operators</i> (to prevent future reviews of identical log entries). b. CONTINUE with the next diagnostic procedure. If all applicable procedures have been completed, RETURN to <i>Routine Monitoring</i>.
If Action Required	<ol style="list-style-type: none"> 5. If the event was not authorized: <ol style="list-style-type: none"> a. DOCUMENT in Security Log. b. GO TO Section A.3, A.3.1 <i>Integrity Checks Table</i>. (See recommended checks below.) LOCATE Integrity Check associated with the asset affected by the event (example: printer, workstation, HMI, etc.), and EXECUTE integrity checks. <p style="margin-left: 20px;">Recommended Checks:</p> <ul style="list-style-type: none"> A.3.2.2 Server/Workstation Log Review A.3.2.6 Server/Workstation Registry Check (MS Windows Only) A.3.2.7 Switch/Router Integrity Check A.3.2.10 Firewall Integrity Check A.3.2.11 Firewall Log Review A.3.2.12 Other Network Device Integrity Check A.3.2.14 IDS Integrity Check A.3.2.16 Peripherals Integrity Check A.3.2.17 Server/Workstation Additional Checks A.3.2.9 Controller Integrity Check A.3.2.1 Server/Workstation Process Check

A.2.13 Network Anomalies: Firewall Log Indicates Anomalous Event Occurred

6. Once you have completed all appropriate Integrity Checks, **GO TO** section
A.2.29 Action Step.

A.2.14 Network Anomalies: Firewall Exhibiting Unusual Behavior

- **Functional Area:** IT or ICS
- **Description:** Firewall
 1. Firewall does not log or alert
 2. Keyboard is locked (host-based firewall)
 3. Spontaneous firewall reboots
 4. Display screen changes for no reason (host-based firewall)
 5. Any other unusual symptom (e.g. host-based firewall is turned off, is suspended, fails, or corresponding service won't start)

Step	Procedures
Investigation	<p>1. CONDUCT trouble-shooting procedures to determine if the firewall is experiencing hardware or software malfunction or network communications issue.</p>
No Action Required	<p>2. If the problem was a routine equipment malfunction or network communications issue:</p> <ol style="list-style-type: none"> a. DOCUMENT the Severity Level as None (0) in the Security Log. b. CONTINUE with the next diagnostic procedure. If all applicable procedures have been completed, RETURN to <i>Routine Monitoring</i>.
If Action Required	<p>3. If the firewall problem is not a routine equipment malfunction:</p> <ol style="list-style-type: none"> a. DOCUMENT in Security Log. b. GO TO Section A.3, A.3.1 <i>Integrity Checks Table</i>. (See recommended checks below.) LOCATE the integrity check associated with the affected firewall. EXECUTE the integrity checks. <p>Recommended Checks:</p> <ul style="list-style-type: none"> A.3.2.1 Server/Workstation Process Check (for host-based firewalls) A.3.2.2 Server/Workstation Log Review (for host-based firewalls) A.3.2.10 Firewall Integrity Check A.3.2.11 Firewall Log Review A.3.2.13 Server/Workstation Rootkit Check (for host-based firewalls) <p>4. Once you have completed all appropriate Integrity Checks, GO TO section A.2.29 Action Step.</p>

A.2.15 Network Anomalies: Abnormal Peripheral Device Communications

- **Functional Area:** IT or ICS
- **Description:** A peripheral device (such as a printer, fax machine, copier, repeaters, hubs, converters, etc.) is attempting to communicate with devices that it normally does not communicate with, uses a service which is not typical, or is communicating abnormally (e.g. scans other devices within the network, “beacons” to an external IP address)

Step	Procedures
Investigation	<ol style="list-style-type: none"> 1. OBTAIN FMC baseline topology. 2. LOCATE the device sending traffic. 3. DETERMINE if the device was reconfigured or replaced and that the change was intentional and conducted by an authorized person.
No Action Required	<ol style="list-style-type: none"> 4. If the device communications are authorized: <ol style="list-style-type: none"> a. DOCUMENT the Severity Level as None (0) in the Security Log. b. CONTINUE with the next diagnostic procedure. If all applicable procedures have been completed, RETURN to <i>Routine Monitoring</i>.
If Action Required	<ol style="list-style-type: none"> 5. If the device communications are not authorized: <ol style="list-style-type: none"> a. DOCUMENT in Security Log. b. GO TO Section A.3, A.3.1 <i>Integrity Checks Table</i>. (See recommended checks below.) EXECUTE the integrity check associated with the device (example: printer, fax, modem, repeater, converters, etc.). <p>Recommended Checks:</p> <ul style="list-style-type: none"> A.3.2.16 Peripherals Integrity Check A.3.2.4 Server/Workstation Communications Check A.3.2.2 Server/Workstation Log Review A.3.2.9 Controller Integrity Check A.3.2.1 Server/Workstation Process Check 6. Once you have completed all appropriate Integrity Checks, GO TO section A.2.29 Action Step.

A.2.16 Network Anomalies: IP Address Originating From Two Or More MAC Addresses

- **Functional Area:** IT or ICS
- **Description:** In general, every device has a single MAC address and single IP address. This type of anomaly could either be devices that are failing and have been replaced with new hardware, or an attacker is spoofing an IP address.

Step	Procedures
Investigation	<ol style="list-style-type: none"> 1. OBTAIN FMC Baseline Topology. 2. LOCATE the device you are investigating. 3. DETERMINE if the device was replaced with new hardware and the IP address was not configured correctly.
No Action Required	<ol style="list-style-type: none"> 4. If the anomalous event can be explained by authorized activities: <ol style="list-style-type: none"> a. DOCUMENT the Severity Level as None (0) in the Security Log. b. CONTINUE with the next diagnostic procedure. If all applicable procedures have been completed, RETURN to <i>Routine Monitoring</i>.
If Action Required	<ol style="list-style-type: none"> 5. If the anomalous event cannot be explained by authorized activities: <ol style="list-style-type: none"> a. DOCUMENT in Security Log. b. GO TO Section A.3, A.3.1 <i>Integrity Checks Table</i>. (See recommended checks below.) LOCATE the device you are investigating (example: workstation, HMI, OPC, printer, etc.). EXECUTE the integrity check associated with that device. <p>Recommended Checks:</p> <ul style="list-style-type: none"> A.3.2.4 Server/Workstation Communications Check A.3.2.2 Server/Workstation Log Review A.3.2.16 Peripherals Integrity Check A.3.2.9 Controller Integrity Check A.3.2.1 Server/Workstation Process Check 6. Once you have completed all appropriate Integrity Checks, GO TO section A.2.29 Action Step.

END OF NETWORK ANOMALIES

A.2.17 Field Device: Abnormal Decrease in Control Process Traffic or Loss of Communications

- **Functional Area:** IT or ICS
- **Description:** The normal flow of control traffic appears slower, sluggish, or there is less traffic than normal (for example, polling cycles not executing)

Step	Procedures
Investigation	<ol style="list-style-type: none"> 1. DETERMINE if an authorized activity or hardware/software malfunction is the cause for the decrease in control traffic: <ol style="list-style-type: none"> a. Did a batch process execute? b. Is a device malfunctioning? c. Did a service stop running? 2. If a failure occurred within the ICS equipment, CONDUCT regular troubleshooting activities.
No Action Required	<ol style="list-style-type: none"> 3. If the anomaly can be explained by a malfunction or authorized activity: <ol style="list-style-type: none"> a. DOCUMENT the Severity Level as None (0) in the Security Log. b. CONTINUE with the next diagnostic procedure. If all applicable procedures have been completed, RETURN to <i>Routine Monitoring</i>.
If Action Required	<ol style="list-style-type: none"> 4. If the anomaly cannot be explained by a malfunction or authorized activity: <ol style="list-style-type: none"> a. DOCUMENT in Security Log. b. GO TO Section A.3, A.3.1 <i>Integrity Checks Table</i>. (See recommended checks below). IDENTIFY the field device being investigated. CONDUCT the integrity checks on the device. <p style="margin-left: 20px;">Recommended Checks:</p> <ul style="list-style-type: none"> A.3.2.9 Controller Integrity Check A.3.2.11 Firewall Log Review A.3.2.5 Server/Workstation Unresponsive Check A.3.2.4 Server/Workstation Communications Check 5. Once you have completed all appropriate Integrity Checks, GO TO section A.2.29 Action Step.

A.2.18 Field Device: Unusual Field Device Activity Observed / Reported

- **Functional Area:** IT or ICS
- **Description:** Unless field devices are under manual control, field devices should be exhibiting behavior that is synchronized with the commands sent by the OPC or control server or the HMI. Any anomalous behavior coming from field devices could be hardware malfunctions or communication path malfunctions. However, once these have been ruled out, a cyber incident should be considered as the possible source of the problem.
 1. Lack of correlation between measurements
 2. Devices' settings are not within normal parameters
 3. Abnormal communication between controllers and field devices
 4. Blocked or delayed information passing from controllers to field devices

Step	Procedures
Investigation	<ol style="list-style-type: none"> 1. DETERMINE if a hardware or communications failure is causing the anomaly. CONDUCT hardware/software trouble-shooting.
No Action Required	<ol style="list-style-type: none"> 2. If the anomaly was caused by a hardware or communications failure: <ol style="list-style-type: none"> a. DOCUMENT the Severity Level as None (0) in the Security Log. b. CONTINUE with the next diagnostic procedure. If all applicable procedures have been completed, RETURN to <i>Routine Monitoring</i>.
If Action Required	<ol style="list-style-type: none"> 3. If the anomaly was not related to a hardware or communications malfunction: <ol style="list-style-type: none"> a. DOCUMENT in Security Log. b. GO TO Section A.3, A.3.1 <i>Integrity Checks Table</i>. (See recommended checks below.) EXECUTE the integrity checks. <p style="margin-left: 20px;">Recommended Checks:</p> <ul style="list-style-type: none"> A.3.2.9 Controller Integrity Check A.3.2.1 Server/Workstation Process Check A.3.2.4 Server/Workstation Communications Check A.3.2.11 Firewall Log Review 4. Once you have completed all appropriate Integrity Checks, GO TO section A.2.29 Action Step.

A.2.19 Field Device: Unexpected Changes to Ladder Logic, Code Configurations, Firmware, and Set Points

- **Functional Area:** IT or ICS
- **Description:** Changes to the controller logic within the field device could come from a process that has been altered, a new process that has been implemented, an old process that was removed, or a process that was sabotaged

Step	Procedures
Investigation	<p>1. DETERMINE if the changes in the controller logic were authorized changes.</p>
No Action Required	<p>2. If changes to the controller logic were authorized:</p> <ol style="list-style-type: none"> DOCUMENT the Severity Level as None (0) in the Security Log. CONTINUE with the next diagnostic procedure. If all applicable procedures have been completed, RETURN to <i>Routine Monitoring</i>.
If Action Required	<p>3. If changes to the controller logic were not authorized:</p> <ol style="list-style-type: none"> DOCUMENT in Security Log. IDENTIFY the devices from which controller logic can be changed. GO TO Section A.3, A.3.1 <i>Integrity Checks Table</i>. (See recommended checks below.) LOCATE the integrity checks associated with these devices, and EXECUTE the integrity checks. <p style="padding-left: 20px;">Recommended Checks:</p> <p style="padding-left: 40px;">A.3.2.9 Controller Integrity Check A.3.2.2 Server/Workstation Log Review (for upstream asset) A.3.2.1 Server/Workstation Process Check (for upstream asset)</p> <p>4. Once you have completed all appropriate Integrity Checks, GO TO section A.2.29 Action Step.</p>

A.2.20 Field Device: HMI, OPC, or Control Server Sending False Information

- **Functional Area:** IT or ICS
- **Description:** If false information is sent to the control system, it could be an error, or a malicious attempt to disguise unauthorized changes, or an initiation of inappropriate actions by system operators

Step	Procedures
Investigation	<p>1. DETERMINE if changes to field controller configurations or anomalous commands sent were authorized.</p>
No Action Required	<p>2. If the changes to field controller configurations or anomalous commands were authorized:</p> <ol style="list-style-type: none"> DOCUMENT the Severity Level as None (0) in the Security Log. CONTINUE with the next diagnostic procedure. If all applicable procedures have been completed, RETURN to <i>Routine Monitoring</i>.
If Action Required	<p>3. If the changes to field controller configurations or the anomalous commands sent were not authorized:</p> <ol style="list-style-type: none"> DOCUMENT in Security Log. GO TO Section A.3, A.3.1 <i>Integrity Checks Table</i>. (See recommended checks below.) LOCATE integrity check for the device. EXECUTE the integrity checks. <p>Recommended Checks:</p> <ul style="list-style-type: none"> A.3.2.9 Controller Integrity Check A.3.2.4 Server/Workstation Communications Check A.3.2.5 Server/Workstation Unresponsive Check A.3.2.3 Unauthorized User Account Activity A.3.2.1 Server/Workstation Process Check A.3.2.13 Server/Workstation Rootkit Check <p>4. Once you have completed all appropriate Integrity Checks, GO TO section A.2.29 Action Step.</p>

A.2.21 Field Device: Anomalous Safety Systems Modifications

- **Functional Area:** IT or ICS
- **Description:** Anomalous modifications to the Safety System could come from an error in the system, accidental misconfiguration, or some other explained event. If the change to the Safety System cannot be explained, the changes could be malicious with the intention of damaging the control system.

Step	Procedures
Investigation	<p>1. DETERMINE if the changes to the Safety System were authorized.</p>
No Action Required	<p>2. If the changes to the Safety System were authorized:</p> <ol style="list-style-type: none"> DOCUMENT the Severity Level as None (0) in the Security Log. CONTINUE with the next diagnostic procedure. If all applicable procedures have been completed, RETURN to <i>Routine Monitoring</i>.
If Action Required	<p>3. If the changes to the Safety System were not authorized:</p> <ol style="list-style-type: none"> DOCUMENT in Security Log. GO TO Section A.3, A.3.1 <i>Integrity Checks Table</i>. (See recommended checks below.) LOCATE integrity check for the device. EXECUTE the integrity check. <p>Recommended Checks:</p> <p style="padding-left: 20px;">A.3.2.9 Controller Integrity Check</p> <p>4. Once you have completed all appropriate Integrity Checks, GO TO section A.2.29 Action Step.</p>

END OF FIELD DEVICE ANOMALIES

A.2.22 IDS Alert: Unexpected Patch Update (Not Announced by Vendors)	
<ul style="list-style-type: none"> • Functional Area: IT or ICS • Description: The IDS observed an irregular vendor patch coming from an external source to a device within the ICS. 	
Step	Procedures
Investigation	<p>1. DETERMINE if the patch update was authorized:</p> <ol style="list-style-type: none"> Contact the entity responsible for patching assets on the ICS. Inquire if patch was authorized.
No Action Required	<p>2. If patch was authorized:</p> <ol style="list-style-type: none"> DOCUMENT the Severity Level as None (0) in the Security Log. CONTINUE with the next diagnostic procedure. If all applicable procedures have been completed, RETURN to <i>Routine Monitoring</i>.
If Action Required	<p>3. If patch is not legitimate,</p> <ol style="list-style-type: none"> DOCUMENT in Security Log. OBTAIN FMC Baseline Topology. From the IDS alert, FIND IP address of device targeted by the patch update. IDENTIFY targeted device (example: server, HMI, switch, etc.). LOCATE integrity checks for that device in Section A.3, A.3.1 <i>Integrity Checks Table</i>. (See recommended checks below.) EXECUTE the appropriate integrity checks. <p>Recommended Checks:</p> <p class="list-item-l1">A.3.2.2 Server/Workstation Log Review</p> <p class="list-item-l1">A.3.2.6 Server/Workstation Registry Check (MS Windows Only)</p> <p class="list-item-l1">A.3.2.7 Switch/Router Integrity Check</p> <p class="list-item-l1">A.3.2.10 Firewall Integrity Check</p> <p class="list-item-l1">A.3.2.12 Other Network Device Integrity Check</p> <p class="list-item-l1">A.3.2.14 IDS Integrity Check</p> <p class="list-item-l1">A.3.2.16 Peripherals Integrity Check</p> <p class="list-item-l1">A.3.2.17 Server/Workstation Additional Checks</p> <p class="list-item-l1">A.3.2.9 Controller Integrity Check</p> <p class="list-item-l1">A.3.2.1 Server/Workstation Process Check</p> <p>4. Once you have completed all appropriate Integrity Checks, GO TO section A.2.29 Action Step.</p>

A.2.23 IDS Alert: Asset Communicating With an Undocumented, Unauthorized, or Unknown IP Address	
Step	Procedures
Investigation	<ul style="list-style-type: none"> • Functional Area: IT or ICS • Description: Server, workstation, peripheral, field controller, or intelligent field device communicating with an undocumented, unauthorized, or unknown IP address. Data flow traffic, boundary traffic, or host connections reveal device is communicating with an unknown IP address.
No Action Required	<ol style="list-style-type: none"> 1. CHECK for possible legitimate reasons an asset is connecting to the ICS: <ol style="list-style-type: none"> a. Was a new asset installed on the ICS? b. Is it an authorized maintenance asset? c. Was an asset misconfigured? 2. If the connection is legitimate: <ol style="list-style-type: none"> a. DOCUMENT the Severity Level as None (0) in the Security Log. b. CONTINUE with the next diagnostic procedure. If all applicable procedures have been completed, RETURN to <i>Routine Monitoring</i>.
If Action Required	<ol style="list-style-type: none"> 3. If the connection is not legitimate and the asset is within the ICS boundary: <ol style="list-style-type: none"> a. DOCUMENT in Security Log. b. CONTACT ISSM, PROVIDE details of the event, and REQUEST assistance in locating unauthorized machine (search may require coordination with the command's network engineering team). c. Once the machine is located, if possible, DETERMINE the ownership of the machine. <ol style="list-style-type: none"> (1) If the machine does not belong to your organization, DISCONNECT the machine, and SURRENDER it to the ISSM for investigation. (2) From the original IDS alert, DETERMINE if or what the unauthorized machine was communicating with. (3) If the unauthorized machine was communicating with an ICS asset, LOCATE the asset on the <i>FMC Topology</i>, and DETERMINE the location and type of asset involved with the event. (4) GO TO Section A.3, A.3.1 <i>Integrity Checks Table</i>. LOCATE the integrity checks associated with this event, and EXECUTE the integrity checks. 4. If the connection was not authorized and the asset is not within the ICS: <ol style="list-style-type: none"> a. DOCUMENT in Security Log. b. CONTACT the ISSM and report unauthorized connection. c. REQUEST the ISSM assist in identifying unauthorized IP address. d. REQUEST the ISSM initiate blacklisting of unauthorized IP address at the ICS boundary. e. GO TO Section A.3, A.3.1 <i>Integrity Checks Table</i>. (See recommended check below.) LOCATE ICS asset communicating with unauthorized IP address, and EXECUTE the integrity checks. <p>Recommended Check: Any Integrity Check may be applicable.</p> 5. Once you have completed all appropriate Integrity Checks, GO TO section A.2.29 Action Step.

A.2.24 IDS Alert: Inbound ICS Protocol Traffic From Unknown Or External IP Address	
Step	Procedures
Investigation	<p>1. OBTAIN FMC Baseline Topology diagram, and LOCATE IP address of ICS target devices.</p> <p>2. From a command line, run “netstat -an” and look for any unexpected internally listening ICS ports or any unexpected external connections.</p> <p>2.1 If unusual output is found, run “netstat -bano” (requires command shell with “administrator” permissions or can run “netstat –ano” without admin permissions). Note: the “-bano” options take extra time to run. It is recommended to pipe the output to a file. Using Netstat with these additional switches shows the mappings from network connection to the listening process/application (this is useful for determining if the open port is associated with an authorized process or not).</p> <p>2. IDENTIFY IP address sending ICS protocol traffic (if possible).</p> <p>a. DETERMINE if communications were authorized.</p>
No Action Required	<p>3. If the communication was authorized:</p> <p>a. DOCUMENT the Severity Level as None (0) in the Security Log.</p> <p>b. CONTINUE with the next diagnostic procedure. If all applicable procedures have been completed, RETURN to <i>Routine Monitoring</i>.</p>
If Action Required	<p>4. If the IP address does not belong to a device authorized to communicate with field controllers using ICS protocols:</p> <p>a. DOCUMENT in Security Log.</p> <p>b. CONTACT the ISSM, and report unauthorized connection.</p> <p>c. REQUEST the ISSM assist in identifying unauthorized IP address.</p> <p>d. REQUEST the ISSM initiate blacklisting of unauthorized IP address at the ICS boundary.</p> <p>e. GO TO Section A.3, A.3.1 <i>Integrity Checks Table</i>. (See recommended checks below.) LOCATE the appropriate Integrity Checks for assets affected, and EXECUTE the integrity checks.</p> <p>Recommended Checks:</p> <p style="padding-left: 20px;">A.3.2.15 IDS Alert – Inbound ICS Protocol</p> <p style="padding-left: 20px;">A.3.2.14 IDS Integrity Check</p> <p>5. Once you have completed all appropriate Integrity Checks, GO TO section A.2.29 Action Step.</p>

A.2.25 IDS Alert: Inbound or Outbound HTTP or HTTPS to or From Unknown or External IP Address	
<ul style="list-style-type: none"> Functional Area: IT or ICS Description: HTTP or HTTPS traffic coming or going to an unknown device 	
Step	Procedures
Investigation	<ol style="list-style-type: none"> 1. OBTAINT FMC Baseline Topology diagram. 2. LOCATE IP address of devices involved with the HTTP or HTTPS communications. 3. DETECT unauthorized HTTPS between internal IPs and/or proxy and TOR nodes (or other similar anonymizing and/or C2 infrastructure). <ol style="list-style-type: none"> 3.1 DETECT download of files from TOR (or other similar anonymizing and/or C2 infrastructure). 3.2 DETECT post requests to/from TOR nodes or other similar anonymizing and/or C2 infrastructure. 3.3 DETECT any other HTTP/HTTPS to/from unknown or External IP Address. 4. DETERMINE if the communication is authorized.
No Action Required	<ol style="list-style-type: none"> 4. If the traffic is authorized: <ol style="list-style-type: none"> a. DOCUMENT the Severity Level as None (0) in the Security Log. b. CONTINUE with the next diagnostic procedure. If all applicable procedures have been completed, RETURN to <i>Routine Monitoring</i>.
If Action Required	<ol style="list-style-type: none"> 5. If the HTTP or HTTPS traffic is not authorized: <ol style="list-style-type: none"> a. DOCUMENT in Security Log. b. From the <i>A.3.1 Integrity Checks Table</i> (see recommended checks below) LOCATE the integrity check associated with the asset sending and receiving the HTTP or HTTPS traffic (example: PLC, HMI, workstation, etc.) and EXECUTE the integrity check. <p>Recommended Checks:</p> <ul style="list-style-type: none"> A.3.2.4 Server/Workstation Communications Check A.3.2.7 Switch/Router Integrity Check A.3.2.10 Firewall Integrity Check A.3.2.12 Other Network Device Integrity Check A.3.2.14 IDS Integrity Check A.3.2.16 Peripherals Integrity Check A.3.2.17 Server/Workstation Additional Checks A.3.2.9 Controller Integrity Check 6. Once you have completed all appropriate Integrity Checks, GO TO section A.2.29 Action Step.

A.2.26 IDS Alert: Unexpected Connection to External or Unknown IPs																											
<ul style="list-style-type: none"> • Functional Area: IT or ICS • Description: An ICS field controller is communicating with an unknown device or machine 																											
Step	Procedures																										
Investigation	<p>1. OBTAINT FMC Baseline Topology.</p> <p>2. DETERMINE if a new system was installed or if an authorized user was using a maintenance laptop or other asset to connect to the network.</p> <p>3. Detect outbound ICS, admin, and Windows protocol traffic:</p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">BACnet/IP</td><td style="width: 70%;">UDP 47808</td></tr> <tr> <td>DNP3</td><td>TCP/UDP 20000</td></tr> <tr> <td>EtherCAT</td><td>UDP 34980</td></tr> <tr> <td>EtherNet/IP/CIP</td><td>TCP/UDP 44818, TCP/UDP 2222</td></tr> <tr> <td>FL-net</td><td>UDP 55000-55003</td></tr> <tr> <td>Foundation Fieldbus</td><td>TCP/UDP 1089-1091</td></tr> <tr> <td>IEC 61850</td><td>TCP 102</td></tr> <tr> <td>Modbus</td><td>TCP 502</td></tr> <tr> <td>OPC</td><td>TCP 4840</td></tr> <tr> <td>PROFINET</td><td>TCP/UDP 34962-34964</td></tr> <tr> <td>ssh</td><td>22</td></tr> <tr> <td>telnet</td><td>23</td></tr> <tr> <td>smb</td><td>139 and 445</td></tr> </table>	BACnet/IP	UDP 47808	DNP3	TCP/UDP 20000	EtherCAT	UDP 34980	EtherNet/IP/CIP	TCP/UDP 44818, TCP/UDP 2222	FL-net	UDP 55000-55003	Foundation Fieldbus	TCP/UDP 1089-1091	IEC 61850	TCP 102	Modbus	TCP 502	OPC	TCP 4840	PROFINET	TCP/UDP 34962-34964	ssh	22	telnet	23	smb	139 and 445
BACnet/IP	UDP 47808																										
DNP3	TCP/UDP 20000																										
EtherCAT	UDP 34980																										
EtherNet/IP/CIP	TCP/UDP 44818, TCP/UDP 2222																										
FL-net	UDP 55000-55003																										
Foundation Fieldbus	TCP/UDP 1089-1091																										
IEC 61850	TCP 102																										
Modbus	TCP 502																										
OPC	TCP 4840																										
PROFINET	TCP/UDP 34962-34964																										
ssh	22																										
telnet	23																										
smb	139 and 445																										
No Action Required	<p>3. If the unexpected connection was authorized:</p> <ol style="list-style-type: none"> DOCUMENT the Severity Level as None (0) in the Security Log. CONTINUE with the next diagnostic procedure. If all applicable procedures have been completed, RETURN to <i>Routine Monitoring</i>. 																										
If Action Required	<p>4. If the connection was not authorized:</p> <ol style="list-style-type: none"> DOCUMENT in Security Log. GO TO Section A.3, A.3.1 <i>Integrity Checks Table</i>. (See recommended checks below.) LOCATE and EXECUTE the Integrity Check associated with the affected devices. <p>Recommended Checks:</p> <ul style="list-style-type: none"> A.3.2.15 IDS Alert Inbound ICS Protocol A.3.2.4 Server/Workstation Communications Check A.3.2.16 Peripherals Integrity Check A.3.2.17 Server/Workstation Additional Checks A.3.2.9 Controller Integrity Check <p>5. Once you have completed all appropriate Integrity Checks, GO TO section A.2.29 Action Step.</p>																										

A.2.27 IDS Alert: Unusual Lateral Connections (Connections in the Same Network Segment) Between ICS Assets

<ul style="list-style-type: none"> Functional Area: IT or ICS Description: An ICS device or machine has expanded its communications to other devices or machines within the ICS. 	
Step	Procedures
Investigation	<ol style="list-style-type: none"> 1. OBTAIN FMC Baseline Topology and Data Flow Diagram: <ol style="list-style-type: none"> a. From the IDS Alert, DOCUMENT: <ol style="list-style-type: none"> (1) The IP address of the asset conducting the scans. (2) The IP address of the assets being scanned. b. Using the FMC Baseline topology, IDENTIFY the communication path from the scanning asset to the target asset. c. Using the Data Flow Diagram, DETERMINE if the communication is normal.
No Action Required	<ol style="list-style-type: none"> 2. If the communication is normal: <ol style="list-style-type: none"> a. DOCUMENT the Severity Level as None (0) in the Security Log. b. CONTINUE with the next diagnostic procedure. If all applicable procedures have been completed, RETURN to <i>Routine Monitoring</i>.
If Action Required	<ol style="list-style-type: none"> 3. If the communication is not normal, determine if system's maintenance personnel made authorized changes to the system. If the communication is not authorized: <ol style="list-style-type: none"> a. DOCUMENT in Security Log. b. GO TO Section A.3, A.3.1 <i>Integrity Checks Table</i>. (See recommended checks below.) LOCATE the Integrity Check associated with the affected devices (example: PLC, printer, HMI, switch, workstation, etc.). EXECUTE the integrity checks on the affected devices. <p style="padding-left: 20px;">Recommended Checks:</p> <ul style="list-style-type: none"> A.3.2.4 Server/Workstation Communications Check A.3.2.16 Peripherals Integrity Check A.3.2.17 Server/Workstation Additional Checks A.3.2.9 Controller Integrity Check 4. Once you have completed all appropriate Integrity Checks, GO TO section A.2.29 Action Step.

A.2.28 IDS Alert: All Other Alerts

- **Functional Area:** IT or ICS
- **Description:** IDS can alert on a wide variety of events; some are false positives

Step	Procedures
Investigation	<p>1. OBTAİN FMC Baseline Documentation, Locate asset(s) involved with the alert.</p> <p>2. DETERMINE if the alert is an authorized action.</p>
No Action Required	<p>3. If the alert event was authorized:</p> <ol style="list-style-type: none"> DOCUMENT the Severity Level as None (0) in the Security Log. Mark entry as future IDS rules update (to prevent future alerts). CONTINUE with the next diagnostic procedure. If all applicable procedures have been completed, RETURN to <i>Routine Monitoring</i>.
If Action Required	<p>4. If the alert was not authorized:</p> <ol style="list-style-type: none"> DOCUMENT in Security Log. GO TO Section A.3, A.3.1 <i>Integrity Checks Table</i>. (See recommended checks below.) LOCATE the integrity checks associated with the asset (example: printer, workstation, HMI, PLC, etc.) and EXECUTE the integrity checks. <p>Recommended Checks:</p> <ul style="list-style-type: none"> A.3.2.2 Server/Workstation Log Review A.3.2.6 Server/Workstation Registry Check (MS Windows Only) A.3.2.7 Switch/Router Integrity Check A.3.2.10 Firewall Integrity Check A.3.2.12 Other Network Device Integrity Check A.3.2.14 IDS Integrity Check A.3.2.16 Peripherals Integrity Check A.3.2.17 Server/Workstation Additional Checks A.3.2.9 Controller Integrity Check A.3.2.1 Server/Workstation Process Check <p>5. Once you have completed all appropriate Integrity Checks, GO TO section A.2.29 Action Step.</p>

END OF IDS ALERTS

A.2.29 Action Step	
Action	<ol style="list-style-type: none">1. After completing the appropriate checks, if there are no findings:<ol style="list-style-type: none">a. DOCUMENT the Severity Level as None (0) in the Security Log.b. RETURN to <i>Routine Monitoring</i>.2. After completing the appropriate checks, if you documented a Severity Level of High (3), or the evidence is sufficient to suggest malicious cyber activity, CONTACT the ISSM and PROVIDE the following information:<ol style="list-style-type: none">a. Severity Level of High (3) and/or the Severity Levels of the checks that provided sufficient evidence to justify reportable malicious activity.b. Affected devices.c. IP addresses of devices.d. Description of procedures taken to identify the issue.e. Results of the Integrity Checks that support the Severity Level.f. Significance of affected device.g. REQUEST the ISSM secure permission from the commander to allow <i>Mitigation</i> actions.h. DOCUMENT the preceding information in the Security Log.3. If permission to <i>Mitigate</i> is granted, CONTINUE to the <i>Mitigation</i> section of this TTP.4. If permission to <i>Mitigate</i> is not granted, REQUEST further instructions from the ISSM.

A.3. Integrity Checks

The activities in the Integrity Checks Table appear in order of most often used.

A.3.1 Integrity Checks Table

Section	Activity	Description	Page
A.3.2.1	Server/Workstation Process Check	Review processes to identify malicious activity. Includes data base servers, control servers, HMIs, OPCs, master terminal units (MTUs), and engineering workstations.	A-36
A.3.2.2	Server/Workstation Log Review	Review database servers, HMIs, control server, engineering workstations, OPCs, MTUs, or firewall log file for anomalies.	A-37
A.3.2.3	Unauthorized User Account Activity	Review host log files for user account changes from the baseline.	A-38
A.3.2.4	Server/Workstation Communications Check	Verify network communications to the expected communications based on the baseline.	A-39
A.3.2.5	Server/Workstation Unresponsive Check	Boot from Rescue CD, and use tools to identify problem.	A-40
A.3.2.6	Server/Workstation Registry Check	Identify changes and anomalies in the registry (MS Windows Only).	A-41
A.3.2.7	Switch/Router Integrity Check	Determine if running configuration, startup configuration, or operating system files have been modified.	A-43
A.3.2.8	Validate Data Flow (Network Traffic)	Verify the data flow, and compare to the baseline.	A-44
A.3.2.9	Controller Integrity Check	Where possible, verify the operating system, configuration files, and firmware against the baseline. Includes PLCs, Intelligent electronic device (IED), remote terminal unit (RTU), etc.	A-45
A.3.2.10	Firewall Integrity Check	Determine if configuration files, access control lists, operating system, or log files have been modified.	A-47
A.3.2.11	Firewall Log Review	Review firewall log file for anomalies.	A-49
A.3.2.12	Other Network Devices Integrity Check	Determine if device has configuration files, operating systems, et cetera, and if so, whether they have been modified. Includes converters, hubs, etc.	A-50
A.3.2.13	Server/Workstation Rootkit Check	Check the device for a rootkit.	A-51
A.3.2.14	IDS Integrity Check	Determine if IDS configuration files, rules, operating system, firmware, or log files have been modified.	A-52
A.3.2.15	IDS Alerts – Inbound ICS Protocol	Determine if the communications coming from the originating IP address should be communicating with the destination machines/device.	A-54
A.3.2.16	Peripheral Integrity Check	Where possible, verify the operating system and firmware against the baseline.	A-55
A.3.2.17	Server/Workstation Additional Checks	1. Detect local DNS host file manipulation/unauthorized entries. 2. Perform search for hidden ADS files (MS Windows Only).	A-56

A.3.2. Integrity Check Procedures

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

A.3.2.2 Server/Workstation Log Review

- **Who should do this check:**

The organization or individual responsible for the host or *Routine Monitoring* staff trained to extract log files from the host

- **What is needed for this check:**

1. Host vendor documentation
2. FMC baseline topology
3. FMC baseline applications
4. FMC baseline configurations
5. FMC user accounts
6. FMC data flow

NOTE: This check should be conducted against application log files and event log files

Step	Procedures
1.	<p>REVIEW log files (security logs, application logs, system logs. Reference vendor documentation as needed).</p>
2.	<p>CHECK log entries for anomalies against FMC baseline applications, configurations, authorized connections, and user accounts. Anomalies can include (but are not limited to):</p> <ol style="list-style-type: none"> a. Unusual user activity. b. Unusual file names or additions or deletions. c. Unusually full log files or totally cleared log files or logs out of date sequence. e.g. For Windows: Event log clear results in: System Event ID 104 Security Event ID 1102 d. Unexpected configuration changes. e. Unexpected system halts and reboots logged. e.g. For Windows: Shutdown/Restart results in: System Event ID 1074 Event log start results in: System Event ID 6005 Event log stop results in: System Event ID 6006 Security Event ID 1100 f. File names with unusual characters or files not found in the baseline. g. Unexpected firmware updates. h. Unexpected remote connections. i. Review Windows Security event log for unexpected use of command shell (cmd.exe - EventID 4688) and also PowerShell. Note: By default, opening of a command shell does not generate an event log event. It is possible to adjust Windows policy to log this information, for details see Appendix E, item EE.6 and EE.17. j. Review Windows System and Security event log for unexpected stops/starts/restarts of legitimate services/processes. e.g. For Windows:

A.3.2.1 Server/Workstation Process Check	
	<p>Stopping Windows Firewall Service results in:</p> <ul style="list-style-type: none"> Security Event ID 5025 System Event ID 7036 <p>Starting Windows Firewall Service results in:</p> <ul style="list-style-type: none"> Security Event ID 5024 System Event ID 7036 <p>Event log stop results in:</p> <ul style="list-style-type: none"> System Event ID 6006 Security Event ID 1100 <p>Event log start results in:</p> <ul style="list-style-type: none"> System Event ID 6005
3.	<p>If anomalies are found:</p> <p>DOCUMENT details of the event in Security Log.</p> <p>If malware or evidence of malicious behavior is identified:</p> <ol style="list-style-type: none"> a. DOCUMENT the Severity Level of High (3). b. GO TO section A.2.29 Action Step. <p>If malware or evidence of malicious behavior is not certain:</p> <ol style="list-style-type: none"> a. DOCUMENT the Severity Level of Medium (2). b. If coming from <i>Section A.3.2.1</i>, RETURN to A.3.2.1, otherwise RETURN to the originating diagnostic procedure, and continue with <i>Recommended Checks</i>. Focus on Server/Workstation Checks.
4.	<p>If no anomalies are found:</p> <ol style="list-style-type: none"> a. DOCUMENT the Severity Level of None (0). b. If coming from <i>Section A.3.2.1</i>, RETURN to A.3.2.1, otherwise RETURN to the originating diagnostic procedure, and continue with <i>Recommended Checks</i>.

A.3.2.3 Unauthorized User Account Activity

- Who should do this check: ICS or IT personnel
- What is needed for this check:
 1. Vendor documentation
 2. FMC user accounts

Step	Procedures
1.	ACCESS system log files (such as Windows event log, syslogs, or log files associated with applications).
2.	COMPARE the log files to the FMC <i>User Accounts</i> and look for anomalous user activity (new user, user with elevated privileges, etc.).
3.	If an irregular user was found, or a regular user's access has changed: <ol style="list-style-type: none"> a. DOCUMENT the access anomaly in the Security Log. b. CONTACT system administrator(s) who manages user access for the asset, and ask if the irregular user is an authorized change.
4.	If the access anomaly was not authorized: <ol style="list-style-type: none"> a. DOCUMENT details of the event in Security Log. b. DOCUMENT the Severity Level of High (3). c. GO TO section A.2.29 <i>Action Step</i>.
5.	If no access anomalies were found or no anomalies were authorized: <ol style="list-style-type: none"> a. DOCUMENT the Severity Level as None (0). b. If coming from Section A.3.2.1, RETURN to A.3.2.1, otherwise RETURN to the originating diagnostic procedure and continue with <i>Recommended Checks</i>.

A.3.2.4 Server/Workstation Communications Check

- **Who should do this check:**
The organization or individual responsible for the server or workstation
- **What is needed for this check:**
 1. Retrieve the following FMC baseline files and/or documents:
 - a. FMC data flow chart
 - b. FMC baseline topology
 - c. FMC baseline authorized process and tasks
 - d. FMC baseline software list
 - e. FMC baseline system information
 2. Rescue CD from Jump-Kit (bootable CD with analysis tools)

Step	Procedures
1.	OBTAİN FMC Data Flow Chart.
2.	OPEN a command line from the Windows desktop (If needed, see appendix D reference: National Security Agency (NSA) document <i>Position Zero</i>).
3.	<p>EXECUTE the following command to capture the machine's network status, and store it to a file:</p> <p>c:\> netstat –ano >(drive letter):\asset name-NetStat.txt <i>Example: c:\>netstat –ano > c:\>HMI-BLD1-NetStat.txt</i></p> <p>If NetFlow is available, CHECK the flow of traffic at key points in the network.</p> <p>NetFlow runs on a variety of Cisco routers, adaptive security appliance (ASA) firewalls and switches. Some other vendors, like 3Com and Riverbed also support NetFlow.</p>
4.	OPEN the newly created file using Notepad.
5.	COMPARE network communications to the expected communications for this machine in the <i>FMC Data Flow Chart</i> .
6.	If the machine is communicating irregularly: <ol style="list-style-type: none"> a. DOCUMENT details of the event in Security Log. b. DOCUMENT the Severity Level of High (3). c. GO TO section A.2.29 Action Step.
7.	If no anomalous communications were found: <ol style="list-style-type: none"> a. DOCUMENT the Severity Level as None (0). b. RETURN to the originating diagnostic procedure and continue with <i>Recommended Checks</i>.

A.3.2.5 Server/Workstation Unresponsive Check

- **Who should do this check:**

The organization or individual responsible for the server or workstation.

- **What is needed for this check:**

1. Rescue CD
2. FMC baseline software list
3. FMC baseline system information

Step	Procedures
1.	<p>If system is unresponsive:</p> <ol style="list-style-type: none"> a. INSERT Rescue CD in the drive bay of the machine and REBOOT. <ol style="list-style-type: none"> (1) If needed, perform "hard" reboot by turning the power off and then on. (2) You may need to reconfigure the basic input and output system (BIOS) to allow booting from a CD.
	<p>Note: Servers and workstations may become unresponsive for many reasons, including hardware failure, software conflicts, configuration errors, etc. Perform normal troubleshooting along with the recommended checks to determine if the problem is cyber-related.</p>
2.	<p>PERFORM system diagnostic to determine:</p> <ol style="list-style-type: none"> a. Is there a good Master Boot Record? b. Is there a hardware error? c. Is there a problem with the memory? d. Do the files appear to be accessible?
3.	<p>If malicious or suspicious changes were made on the system:</p> <ol style="list-style-type: none"> a. DOCUMENT details of the event in Security Log. b. CONTACT system administrator responsible for the machine or the command ISSM, and: <ol style="list-style-type: none"> (1) REPORT suspicious change. (2) REQUEST assistance in determining if the change is malicious. (3) If the change is not malicious, CONTINUE to Step 4. (4) If the process is malicious: <ol style="list-style-type: none"> (a) DOCUMENT the Severity Level of High (3) in the Security Log. (b) GO TO section A.2.29 Action Step.
4.	<p>If no malicious or suspicious changes were made on the system:</p> <ol style="list-style-type: none"> a. DOCUMENT the Severity Level as None (0). b. RETURN to the originating diagnostic procedure, and continue with <i>Recommended Checks</i>.

A.3.2.6 Server/Workstation Registry Check (MS Windows Only)

- **Who should do this check:**

The organization or individual responsible for the server or workstation.

- **What is needed for this check:**

Retrieve the following FMC baseline files and/or documents:

1. FMC Baseline Registry
2. Rescue CD from Jump-Kit (Bootable CD with analysis tools)

NOTE: Using *RegEdit*, or any other utility that allows the registry to be modified, can change the configurations and make the system act unusual or even prevent it from running. It is recommended that the *reg query* command or other utility that makes a copy of the registry, or only provides read only access, be used.

Step	Procedures
1.	<p>If the server or workstation is running the Windows operating system, use a registry edit tool to EVALUATE contents of the registry. These are tools and utilities that can be used to access the registry.</p> <ol style="list-style-type: none"> a. <i>Reg query</i> (Windows utility). b. <i>RegEdit</i> (Windows utility). c. SysInternals Registry viewing tool “Autoruns for Windows” (free Windows utilities, but must be installed, see section G.5 for additional information). <p>Note: Be sure to adjust Sysinternals' Autoruns "Options" to uncheck "Hide Windows Entries" (or some of the keys shown in step 2 will not appear)</p> <ol style="list-style-type: none"> d. RegRipper (free administrator utility). e. NirSoft (free administrator utility). f. OSForensics (free administrator utility).
2.	<p>EVALUATE the following keys using the <i>reg query</i> command from the command prompt:</p> <p>(If needed, see Appendix E: Technical Supplement, section EE.1 Check Windows Registry “Run” Keys).</p> <ol style="list-style-type: none"> a. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run This key runs EVERY time the system is booted. b. HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run This key runs EVERY time that specific user logs in. c. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce This key runs ONCE when the system is booted, and then the OS will remove it from the registry. d. HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce This key runs once when that user logs in and then the OS will remove it from the registry. e. HKLM\System\MountedDevices Mounted Devices.

A.3.2.6 Server/Workstation Registry Check (MS Windows Only)	
	<p>f. HKLM\System\CurrentControlSet\Enum\USBSTOR USB Devices that have been connected to the system.</p> <p>g. HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs Most recently used documents.</p> <p>h. HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU Commands executed by the Start Run options from the Start menu.</p> <p>i. HKCU\Software\Microsoft\Internet Explorer\TypedURLs URLs the user has typed into the address bar.</p> <p>j. HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDLg32\OpenSavePidIMRU Files accessed by the Open or Save dialog boxes.</p>
3.	EVALUATE the values for each of the inspected keys. DETERMINE if the value is valid or invalid.
4.	If invalid and/or malicious entries were found: <ol style="list-style-type: none"> DOCUMENT the details of the event in the Security Log. DOCUMENT the Severity Level of High (3). GO TO section A.2.29 Action Step.
5.	If no anomaly was found: <ol style="list-style-type: none"> DOCUMENT the Severity Level as None (0). RETURN to the originating diagnostic procedure and continue with <i>Recommended Checks</i>.

A.3.2.7 Switch/Router Integrity Check

- **Who should do this check:**
Individual responsible for managing the router or switch
- **What is needed for this check:**
 1. FMC router or switch operating system hash value
 2. FMC router or switch configuration files
 3. FMC router or switch instructions for extracting configuration files and operating system hash values

Step	Procedures
1.	<p>ENSURE the operating system version of the FMC hash files are the same as the device you are evaluating.</p> <p>If they are different, GO TO the vendor's web site, and DOWNLOAD the latest FMC hash files for the device you are evaluating.</p>
2.	Using local procedures, COPY running-config and startup-config from the switch or router to a location where these files can be compared to the FMC baseline configuration files.
3.	COMPARE the FMC operating system hash value to the extracted operating system hash value.
4.	If the value of the FMC operating system hash value and the extracted hash value are not the same: <ol style="list-style-type: none"> a. CONTACT networking staff and ask if any authorized changes. b. DOCUMENT response in the Security Log.
5.	COMPARE the FMC configuration to the configuration extracted from the device.
6.	If the configurations have changed: <ol style="list-style-type: none"> a. CONTACT networking staff, and verify the validity of the changes. b. DOCUMENT change in the Security Log.
7.	If either the hash value of the operating system or the configuration file has changed, and these were not authorized: <ol style="list-style-type: none"> a. DOCUMENT the Severity Level of High (3). b. On the <i>FMC Topology Diagram</i>, LOCATE devices connecting to the affected device. c. GO TO section A.2.29 Action Step.
8.	If any changes to the hash value of the operating system or configuration files were authorized, or if no changes were found: <ol style="list-style-type: none"> a. DOCUMENT the Severity Level as None (0). b. RETURN to the originating diagnostic procedure, and continue with <i>Recommended Checks</i>.

A.3.2.8 Validate Data Flow (Network Traffic)

- **Who should do this check:**
The person responsible for IT within the ICS organization
- **What is needed for this check:**
 1. Instructions on capturing network traffic (or data flows) on your network
 2. FMC Baseline Topology
 3. FMC Data Flow Diagram

Step	Procedures
1.	RETRIEVE Baseline Data Flow Table and the ICS Topology.
2.	LOCATE the devices you are investigating by IP address on the Data Flow Table and on the FMC Baseline Topology.
3.	Using the FMC Baseline Topology, IDENTIFY the communications path between the devices you are investigating.
4.	DOCUMENT all the devices along the communication path.
5.	On the Baseline Data Flow Table, LOCATE the devices you are investigating as well as the devices in between the devices you are investigating.
6.	DOCUMENT the ports, protocols, and services authorized on the Data Flow Table (these are your ports protocols and services that SHOULD be seen along this communications path).
7.	Using the methodology selected for your site, LOCATE the point along the communication path of the devices that you are investigating which will allow you to capture the data flow (also called NetFlows or network traffic).
8.	ESTABLISH your capture point and begin data flow capture.
9.	OBSERVE data flow for anomalous traffic (anomalous traffic includes ports, protocols, and services that are not included in the Baseline Data Flow Table).
10.	If anomalous traffic is not immediately observed, and the event in question is coming from an IDS Alert, ALLOW data flow capture to run for at least 24 hours.
11.	If anomalous traffic is found: <ol style="list-style-type: none"> a. DOCUMENT details of the event in the Security Log. b. IDENTIFY the originating asset and the destination asset's IP address. c. LOCATE the assets involved with the event on the ICS topology. d. DETERMINE the type of asset involved with the incident. e. GO TO A.3.1 Integrity Checks Table, and locate the integrity check for those assets. CONDUCT the checks.
12	If no anomalous traffic was found: <ol style="list-style-type: none"> a. DOCUMENT the Severity Level as None (0). b. RETURN to the originating diagnostic procedure and continue with <i>Recommended Checks</i>.

A.3.2.9 Controller Integrity Check

- **Who should do this check:**

The organization or individual responsible for the integrity of field controllers

- **What is needed for this check:**

1. FMC field controller configuration files
2. FMC baseline topology
3. Field controller vendor documentation
4. Jump-Kit

Step	Procedures
1.	If the controller contains log files, REVIEW the log files for anomalies.
2.	USE Jump-Kit as appropriate.
3.	COMPARE state of field device with field controller settings. May include: <ol style="list-style-type: none"> a. CHECK to see if Mode is correct. b. CHECK lights and indicators.
4.	Connect the Jump-Kit computer to the device.
5.	If possible, RETRIEVE the field controllers FMC configuration files. If not possible, GO TO Step 10.
6.	EXTRACT configuration files from field controller.
7.	COMPARE extracted configuration file to FMC configuration file.
8.	If the values match and there is no change in the mode, and the log files do not contain anomalies: <ol style="list-style-type: none"> a. DOCUMENT the Severity Level as None (0). b. EXIT procedure, RETURN to the originating diagnostic procedure and continue with <i>Recommended Checks</i>.
9.	If the values do not match, DOCUMENT in the Security Log.
10.	On the baseline topology, IDENTIFY which HMI is communicating with the field controller.
11.	CONTACT the operator of that HMI, and brief operator on status of controller.
12.	REQUEST the HMI operator COMPARE the configuration settings recorded in the HMI with those of the field controller.
13.	DOCUMENT HMI operator's response in Security Log.
14.	RECOMMEND HMI operator review the HMI application (whether the values between the controller match).
15.	VALIDATE the set points and operating condition of the field device connected to the field controller.
16.	If an anomaly is identified from the previous steps: <ol style="list-style-type: none"> a. DOCUMENT details of the event in the Security Log. b. DOCUMENT the Severity Level of High (3). c. GO TO section A.2.29 Action Step.

A.3.2.9 Controller Integrity Check

- | | |
|-----|--|
| 17. | <p>If anomaly does not exist:</p> <ul style="list-style-type: none">a. DOCUMENT the Severity Level as None (0)b. RETURN to the originating diagnostic procedure and continue with <i>Recommended Checks</i>. |
|-----|--|

A.3.2.10 Firewall Integrity Check

- **Who should do this check:**
Individual responsible for firewall administration
- **What is needed for this check:**
 1. FMC firewall configuration
 2. FMC access control list (ACL)
 3. FMC hash value for firewall operating system and firmware
 4. Firewall documentation
 5. ICS topology diagram

Step	Procedures
1.	<p>LOCATE extraction procedures from the vendor documentation for the following files:</p> <ol style="list-style-type: none"> a. Configurations b. Access Control Lists c. Hash values for operating system d. Hash values for firmware e. Log file
2.	Using local procedures, COPY running-config and startup-config, and identify firmware version of the firewall to a location that will enable the comparison of these files and version level to the FMC baseline files and version.
3.	<p>ENSURE the operating system and firmware versions of the FMC hash values are the same as the machine hash values you are evaluating. If the values are different, GO TO the vendor's web site. LOOKUP the hash values for the operating system and firmware versions installed on the machine you are evaluating (the vendor should have a history of hash values), and UPDATE FMC baseline.</p>
4.	<p>COMPARE:</p> <ol style="list-style-type: none"> a. FMC configuration files against extracted configuration files. b. FMC ACL to extracted ACL. c. FMC hash values for operating system to firewall operating system hash value. d. FMC hash value for firmware and the firewall operating system and firmware. <p>CHECK log file for anomalies:</p> <ol style="list-style-type: none"> a. Unusual users or activities. b. Time stamp anomalies. c. Deleted or modified log file.
5.	If the extracted configurations, ACL, or hash values are different from the FMC baseline, or if the log file exhibits anomalies, CONTACT networking staff and VALIDATE changes: <ol style="list-style-type: none"> a. Did network staff change configuration files? b. Did network staff change the ACLs? c. Was the operating system upgraded? d. Was new hardware installed?
6.	If the extracted log files anomalies, configuration, ACL, or hash value changes were not authorized: <ol style="list-style-type: none"> a. DOCUMENT details of the event in the Security Log. b. DOCUMENT the Severity Level of High (3).

A.3.2.10 Firewall Integrity Check	
	<p>c. Using the <i>ICS topology diagram</i>, LOCATE machines/devices connected to the firewall.</p> <p>d. NOTIFY additional ICS personnel that the integrity of connecting machines/devices should be checked.</p> <p>e. GO TO section A.2.29 Action Step.</p>
7.	<p>If no anomalies were found:</p> <p>a. DOCUMENT the Severity Level as None (0).</p> <p>b. RETURN to the originating diagnostic procedure, and continue with <i>Recommended Checks</i>.</p>

A.3.2.11 Firewall Log Review

<ul style="list-style-type: none"> ● Who should do this check: The organization or individual responsible for the firewall administration, or Routine Monitoring staff trained to extract log files from the firewall ● What is needed for this check: <ol style="list-style-type: none"> 1. Firewall vendor documentation 2. FMC baseline topology 	
Step	Procedures
1.	EXTRACT firewall log (reference vendor documentation as needed).
2.	CHECK log entries for anomalies. Anomalies can include (but are not limited to): <ol style="list-style-type: none"> a. Inbound SMTP traffic (email) destined for an ICS asset, such as the HMI, Historian, Application Server, etc. b. Inbound or outbound ICS protocol traffic. This could include MODBUS or DNP3, etc. c. Inbound or outbound Telnet, FTP, TFTP, HTTP. d. Unscheduled firmware pushes or pulls for ICS or SCADA devices, unexpected data transfers, or any other communications with IP addresses that are not clearly known to the IT and/or ICS manager.
3.	If anomalies are found: <ol style="list-style-type: none"> a. IDENTIFY the destination IP for the anomalous traffic. b. DOCUMENT details of the event in the Security Log. c. DOCUMENT the Severity Level of High (3). d. Using the <i>FMC Baseline Topology</i>, LOCATE destination device by its IP address. e. DOCUMENT the device type of the destination traffic in the Security Log. f. CONTACT operators of the destination devices, and convey your findings. g. RECOMMEND operators conduct an Integrity Check of the devices. h. STAND BY to assist operators as necessary. i. GO TO section A.2.29 Action Step.
4.	If no anomalies are found: <ol style="list-style-type: none"> a. DOCUMENT the Severity Level as None (0). b. RETURN to the originating diagnostic procedure and continue with <i>Recommended Checks</i>.

A.3.2.12 Other Network Devices Integrity Check

- **Who should do this check:**

The organization or individual responsible for network administration

- What is needed for this check:**

1. FMC operating system hash value
2. FMC firmware hash value (not available for all devices)
3. FMC network device configuration files
4. FMC baseline topology
5. Vendor documentation

Step	Procedures
1.	RETRIEVE the network device's FMC configuration files, operating system hash value and firmware hash values (not available for all devices).
2.	EXTRACT configuration files from network device.
3.	COMPARE extracted configuration file to FMC configuration file.
4.	If the values do not match, DOCUMENT in the Security Log.
5.	RETRIEVE FMC hash value for operating system.
6.	EXTRACT hash value for network device operating system (refer to vendor documentation).
7.	COMPARE the FMC operating system hash value to the extracted hash value.
8.	If the values are different, DOCUMENT difference in Security Log.
9.	If the network device has an FMC firmware hash value, RETRIEVE this value.
10.	EXTRACT firmware hash value from the network device (refer to vendor documentation).
11.	COMPARE the FMC firmware hash value to the extracted hash value. Document the differences in Security Log.
12.	REVIEW the differences found in the Security Log.
13.	If the configuration files are different, DETERMINE if the changes were authorized.
14.	If the hash values were different, DETERMINE if the operating system or firmware was recently upgraded or patched.
15.	If any of the changes were not authorized: <ol style="list-style-type: none"> a. DOCUMENT details of the event in the Security Log. b. DOCUMENT the Severity Level of High (3). c. Using the FMC Topology Diagram, DETERMINE what devices connect to this device. d. Contact operators of connecting devices, and RECOMMEND they conduct an Integrity Check of the connecting devices. e. GO TO section A.2.29 Action Step.
16.	If all changes found were authorized: <ol style="list-style-type: none"> a. DOCUMENT the Severity Level as None (0). b. RETURN to the originating diagnostic procedure and continue with <i>Recommended Checks</i>.

A.3.2.13 Server/Workstation Rootkit Check

- **Who should do this check:**
The organization or individual responsible for the server or workstation
- **What is needed for this check:**
 1. Retrieve the following FMC baseline files and/or documents:
 - a. FMC data flow chart
 - b. FMC baseline topology
 - c. FMC baseline authorized process and tasks
 - d. FMC baseline software list
 - e. FMC baseline system information
 2. Rescue CD from Jump-Kit (bootable CD with analysis tools)

Step	Procedures
1.	CAPTURE volatile memory forensics if possible.
2.	Update the rootkit removal software if necessary, and create new rescue CD.
3.	INSERT the rescue CD into drive bay. REBOOT to launch rootkit removal from the rescue CD.
4.	FOLLOW the directions on the screen. NOTE: Most rootkit removal tools will examine the disk and run for 15 minutes or more depending on the size of your disk. It scans not only the operating system files but also the boot loader and other files, looking for signs of infection.
5.	If a rootkit was found: <ol style="list-style-type: none"> a. DOCUMENT the details of the event in the Security Log. b. DOCUMENT the Severity Level of High (3). c. DETERMINE what the machine is communicating with using the <i>FMC Baseline Topology Diagram</i>. d. GO TO section A.2.29 Action Step.
6.	If no rootkit was found: <ol style="list-style-type: none"> a. DOCUMENT the Severity Level as None (0). b. RETURN to the originating diagnostic procedure and continue with <i>Recommended Checks</i>.

A.3.2.14 IDS Integrity Check

- **Who should do this check:**
The organization or individual responsible for the IDS administration
- **What is needed for this check:**
 1. FMC IDS configuration
 2. FMC rules
 3. FMC hash value for IDS operating system and firmware
 4. IDS documentation
 5. Log file

Step	Procedures
1.	LOCATE extraction procedures from the IDS documentation for the following files: <ol style="list-style-type: none"> a. Configurations. b. Access control lists. c. Hash values for operating system. d. Hash values for firmware.
2.	Using local procedures, COPY the configuration files, access control lists, firmware version, and any appropriate operating system files of the IDS to a location that will enable the comparison of these files and version level to the FMC baseline files and version.
3.	ENSURE the operating system and firmware versions of the FMC hash values are the same as the machine hash values you are evaluating. If the values are different, GO TO the vendor's web site. LOOKUP the hash values for the operating system and firmware versions installed on the machine you are evaluating (the vendor should have a history of hash values), and update FMC baseline.
4.	COMPARE: <ol style="list-style-type: none"> a. FMC configurations to the extracted configurations. b. FMC ACL to extracted ACL. c. FMC operating system hash values to the extracted operating system hash values. d. FMC firmware hash values to the extracted firmware hash values.
5.	If the extracted configurations, ACLs, or hash values are different, CONTACT networking staff and VALIDATE changes: <ol style="list-style-type: none"> a. Did network staff change configuration files? b. Did network staff change the ACLs? c. Was the operating system upgraded? d. Was new hardware installed?
6.	If the extracted configurations, ACLs, or hash value changes were not authorized: <ol style="list-style-type: none"> a. DOCUMENT details of the event in the Security Log. b. DOCUMENT the Severity Level of High (3). c. GO TO section A.2.29 Action Step.

A.3.2.14 IDS Integrity Check

- | | |
|----|---|
| 7. | <p>If no changes to the extracted hash values or files were found:</p> <ul style="list-style-type: none">a. DOCUMENT the Severity Level as None (0).b. RETURN to the originating diagnostic procedure, and continue with <i>Recommended Checks</i>. |
|----|---|

A.3.2.15 IDS Alerts – Inbound ICS Protocol

- **Who should do this check:**
The organization or individual responsible for the IDS administration or individuals trained to conduct Routine Monitoring checks on IDS
- **What is needed for this check:**
 1. IDS vendor documentation
 2. FMC baseline topology
 3. FMC data flow diagram

Step	Procedures
1.	Using the <i>FMC Topology Diagram</i> , LOCATE origin and the destination of the traffic (if the IP address of the origin is outside the ICS boundary, CONTACT the network administrator for assistance).
2.	Using the Baseline Data Flow Diagram, DETERMINE if the communications coming from the originating IP address should be communicating with the destination machines/device.
3.	DETERMINE what protocols should be used between those machines/devices.
4.	If the two machines or devices should not communicate, or the protocol traffic is anomalous: <ol style="list-style-type: none"> a. DOCUMENT details of the event in the Security Log. b. DOCUMENT the Severity Level of High (3). c. GO TO section A.2.29 Action Step.
5.	If the communications are authorized: <ol style="list-style-type: none"> a. DOCUMENT the Severity Level as None (0). b. RETURN to the originating diagnostic procedure and continue with <i>Recommended Checks</i>.

A.3.2.16 Peripheral Integrity Check

- **Who should do this check:**
The organization or individual responsible for the peripheral administration within the ICS boundary
- **What is needed for this check:**
 1. FMC peripheral operating system hash value (if possible)
 2. FMC baseline topology
 3. FMC baseline configurations for peripheral
 4. FMC data flow diagram
 5. Peripheral vendor instructions for extracting configuration files and operating system hash value
 6. Jump-Kit

Step	Procedures
1.	CONNECT Jump-Kit machine to the device.
2.	EXTRACT hash values of the peripheral software and/or firmware (if possible).
3.	EXTRACT configuration files in accordance with the vendor documentation (if possible).
4.	COMPARE extracted hash values of the peripheral software and firmware to the FMC values.
5.	COMPARE extracted configuration files to the FMC configuration files obtained from the baseline.
6.	If anomalies are found in the hash values, VALIDATE that the version of FMC peripheral operating system and the operating system of the device match. <ol style="list-style-type: none"> a. If the operating system version numbers (FMC and device) are not the same, GO TO vendor web site, and OBTAIN the hash value for the operating system the peripheral is using. b. RECHECK hash values using the newly downloaded hash as the new FMC hash value.
7.	If anomalies were found in either the hash values or the configuration files: <ol style="list-style-type: none"> a. DETERMINE the device's communication path using <i>FMC Topology</i> and the <i>FMC Data Flow Diagram</i>. b. NOTIFY operators of devices communicating with this peripheral that the peripheral may have cyber activity, and that they should conduct Integrity Checks of their devices. c. DOCUMENT details of the event in the Security Log. d. DOCUMENT the Severity Level of High (3). e. GO TO section A.2.29 Action Step.
8.	If no anomalies were found: <ol style="list-style-type: none"> a. DOCUMENT the Severity Level as None (0). b. RETURN to the originating diagnostic procedure and continue with <i>Recommended Checks</i>.

A.3.2.17 Server/Workstation Additional Checks (MS Windows Only)

- **Who should do this check:**
The organization or individual responsible for the server or workstation
- **What is needed for this check:**
 1. Retrieve the following FMC baseline files and/or documents:
 - a. FMC hash value for local Windows host file
 - b. FMC baseline software list
 2. Rescue CD from Jump-Kit (bootable CD with analysis tools)

Step	Procedures - DNS Local Host File
1.	<p>Local DNS Host file integrity check:</p> <p>(If needed, see Appendix E: Technical Supplement, section EE.2 Check Integrity of Local DNS Host File, and section EE.3 Check Local DNS Host file registry path).</p> <p>a. DETERMINE if the local DNS host file has any unauthorized entries. Run a hash on the host file (C:\%systemroot%\System32\drivers\etc\hosts) and compare to the hash of a known good host file (from the same OS/version/patch level) to see if they match. If the hashes do not match, review the contents of the host file for any unauthorized entries.</p> <p>b. Using the 'reg query' command CHECK the following registry key: HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters REVIEW the returned string value of: DataBasePath. This string value should = %SystemRoot%\System32\drivers\etc If this value is different, DETERMINE if value is authorized and also REVIEW the contents of the host file (at the specified location) for any unauthorized entries.</p>
2.	<p>Detection of an Alternate Data Streams (ADS) file.</p> <p>(If needed, see Appendix E: Technical Supplement, section EE.4 Hidden Alternate Data Stream (ADS) files).</p> <p>a. Run the Microsoft Sysinternals "Streams" utility, or alternately, run the following native command from the command line to SEARCH for unauthorized ADS files: Dir /R /s c:\[folder path] >> output.txt e.g. Dir /R /s c:\windows\temp >> output.txt</p> <p>b. SEARCH output.txt for entries containing the following string: :\$DATA (This string indicates the presence of an ADS file)</p> <p>NOTE: ADS files can have legitimate uses - in order to reduce false positives, review the content of any suspect ADS files to determine validity.</p>

A.3.2.17 Server/Workstation Additional Checks (MS Windows Only)	
<ul style="list-style-type: none"> • Who should do this check: The organization or individual responsible for the server or workstation • What is needed for this check: <ol style="list-style-type: none"> 1. Retrieve the following FMC baseline files and/or documents: <ol style="list-style-type: none"> a. FMC hash value for local Windows host file b. FMC baseline software list 2. Rescue CD from Jump-Kit (bootable CD with analysis tools) 	
3.	If either an unauthorized host file change and/or an unauthorized ADS file was found: <ol style="list-style-type: none"> a. DOCUMENT the details in the Security Log. b. DOCUMENT the Severity Level of High (3). c. DOCUMENT the specific unauthorized host file information (name/IP address entries/different file path specified) and/or the specific ADS file (name/location). d. GO TO section A.2.29 Action Step.
4.	If no unauthorized entries and/or files were found: <ol style="list-style-type: none"> a. DOCUMENT the Severity Level as None (0). b. RETURN to the originating diagnostic procedure and continue with <i>Recommended Checks</i>.
Step	Procedures – Detection of suspicious strings
1.	Use the Windows Findstr utility to search for strings of interest (suspicious strings may be gleaned from reporting or from online services). <p style="margin-left: 40px;"><u>findstr /s /i “[target text]” [in file or file wildcard]</u></p> <p style="margin-left: 40px;">e.g. C:\temp\search>findstr /s /i /x "needle" *.* test\haystack.txt:needle</p>

ENCLOSURE B: MITIGATION PROCEDURES

B.1. Mitigation Segmentation

Before continuing with the Recovery Procedures, ensure that permission has been obtained from the ISSM or other equal or higher authority. Please be aware that Mitigation may be disruptive to operations and may require additional resources.

The Network Mitigation Segmentation process will be determined by the specific network architecture of the affected network. This process is dependent on the following:

- Locating connections in the network which provide interconnection between separate functional networked sub-systems, enclaves, or layers. (Refer to enclosure E for guidance in assessing the Baseline configuration of your network to aid in locating these connections.)
- Maintaining the functionality of the ICS end process with Network Mitigation Segmentation in place.

Mitigation Segmentation	
Step	Mitigation Segmentation Procedure
1.	<p>LOCATE all connections in your network which reside on the boundaries of your sub-system, enclave, or layer. Refer to your FMC Baseline to assist in determining the location of these connections. DETERMINE the following:</p> <p>The points in your network where a connection exists which provide a potential communications path for malicious external command and control of the system (for example, connections which lead to the Internet, at a switch, firewall, or router).</p> <p style="text-align: center;">AND/OR</p> <p>The points in your network where a connection exists to adjacent networks which provide a potential communications path for malware to propagate between the adjacent networks or sub-systems.</p>
2.	Communication paths to the Internet can be utilized for malicious external command and control. DISCONNECT the network cable(s) connecting the network to the Internet.
3.	Communication paths to adjacent networks or sub-systems can provide a communications path for malware to propagate. DISCONNECT the network cable(s) connecting to adjacent networks or sub-systems.
4.	DOCUMENT all actions taken in the Security Log for after-incident analysis.
5.	Closely MONITOR the operation of the ICS process(es). If any adverse effects are noted as a result of the network isolation, RECONNECT the network and continue to closely MONITOR for adverse impacts. Otherwise, CONTINUE to the next step.

Step	Mitigation Segmentation Procedure
6.	Once the <i>Mitigation</i> is complete, CONTACT the ISSM to provide notification that <i>Mitigation</i> Segmentation has been performed and necessary operations are under local control.
7.	PROCEED to B.2 <i>IT/Network Asset Mitigation</i> and/or B.3 ICS Control Device <i>Mitigation</i> .

B.2. IT/Network Assets

Utilize the IT/Network Device Mitigation Procedure when the affected device(s) discovered during Detection is not directly connected to, or controlling, the ICS process. (Typical equipment such as switches, routers, firewalls, servers, and workstations.)

The main goal of the IT/Network Assets Mitigation is to isolate the infected assets and maintain operation and control of the critical ICS process(es).

IT/Network Device Mitigation	
Step	Mitigation Procedure
1.	When possible, MAINTAIN POWER to the affected devices during this procedure. This will aid in after-incident forensic analysis of the cyber event.
2.	When possible, and unless otherwise directed, PRESERVE forensic data on the affected device(s). Technical assistance may be required to save the data. For details see Enclosure G: Data Collection for Forensics.
3.	DOCUMENT all actions taken in the Security Log for after-incident analysis.
4.	If installed, SWITCH control to the secondary or redundant control network, and MONITOR the operation of the ICS process(es) to ensure the alternate control network is operating properly. If the secondary or redundant control network is functioning properly, PROCEED to the <i>Recovery Procedures</i> in enclosure C for the affected network. If the secondary or redundant control network is not operating properly, PROCEED to the <i>ICS Control Device Mitigation Procedure</i> , enclosure B, section B.3. Otherwise, CONTINUE with the next step.
5.	If no secondary or redundant control network is installed, DISCONNECT the network cable(s) connected to the affected device(s).
6.	After DISCONNECTING the network cable(s) on the affected device(s), closely MONITOR the operation of the ICS process(es) to ensure that there are no adverse effects indicated. If any adverse effects are indicated, PROCEED to the <i>ICS Control Device Mitigation Procedure</i> , enclosure B, section B.3. Otherwise, CONTINUE to the next step.
7.	CONTACT the ISSM to provide notification that the device has been isolated.
8.	PROCEED to the <i>Recovery Procedures</i> in enclosure C.

B.3. ICS Control Device Mitigation

Utilize the ICS Control Device Mitigation Procedure when the affected device(s) is directly controlling the ICS process(es) (typical equipment such as PLCs, RTUs, MTUs, Protective Relay Controllers, Tap Changers, Circuit Breaker Controllers, etc.) or when the IT/Network Device Mitigation Procedure was performed and the ICS process(es) is not functioning properly.

The main goal of the ICS Controller Mitigation Procedure is to isolate the infected device(s) while maintaining operation and control of the ICS-critical process(es).

ICS Control Device Mitigation	
Step	Mitigation Procedure
1.	When possible, MAINTAIN POWER to the affected devices during this procedure. This will aid in after-incident forensic analysis of the cyber event.
2.	When possible and unless otherwise directed PRESERVE forensic data on the affected device(s). Technical assistance may be required to save the data. For details see Enclosure G: Data Collection for Forensics.
3.	DOCUMENT all actions taken in the Security Log for after-incident analysis.
4.	If installed, SWITCH control to the secondary or redundant control network, and MONITOR the operation of the ICS process(es) to ensure the alternate control network is operating properly. If the secondary or redundant control network is functioning properly, PROCEED to the <i>Recovery Procedures</i> in enclosure C for the affected network. If the secondary or redundant control network is not functioning properly, CONTINUE performing these <i>ICS Control Device Mitigation Procedures</i> on the secondary or redundant control network.
5.	DISCONNECT the network cable(s) on the affected ICS Control Device(s), then TAKE LOCAL CONTROL of the affected ICS Control Device.
6.	MONITOR the operation of the ICS process(es) to ensure proper operation. If the ICS Process(es) is NOT OPERATING PROPERLY , or LOCAL CONTROL CANNOT BE MAINTAINED and personnel safety or equipment damage is imminent, SHUT DOWN the system. CONTACT the ISSM for further instructions on how to proceed. Otherwise, PROCEED to the next step.
7.	CONTACT the ISSM to provide notification that the ICS Control Device has been isolated and the system is in local control.
8.	PROCEED to the <i>Recovery Procedures</i> located in enclosure C.

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	
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.

Typical Equipment: Servers/Workstations	
8.	UPDATE the antivirus software (if installed) with the latest update and INITIATE a full system scan.
Reintegration	
9.	<p>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.</p> <p>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 <i>Recovery</i> has been performed on these devices.</p>
10.	<p>When each device in the layer or sub-system has been recovered, RECONNECT all of the devices in the sub-system or layer.</p> <p>DO NOT RECONNECT to the wider network at this time.</p>
11.	VERIFY that the cyber incident artifacts have been eliminated using available Detection tools (IDS, Log Review, NMap, Netstat, Wireshark, etc).
12.	<p>MONITOR the system for anomalous behavior.</p> <p>If anomalous behavior is evident, RETURN to the <i>Detection Procedures</i> (enclosure A) and/or <i>Mitigation Procedures</i> (enclosure B) of this ACI TTP as necessary.</p>
13.	<p>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.</p>
14.	<p>MONITOR the system for anomalous behavior.</p> <p>If anomalous behavior is evident, RETURN to the <i>Detection Procedures</i> (enclosure A) and/or <i>Mitigation Procedures</i> (enclosure B) of this ACI TTP as necessary.</p>
15.	SUBMIT all records of <i>Recovery</i> actions to the ISSM or CPT.
16.	RETURN to <i>Routine Monitoring</i> of the network.

C.2. Recover – Routers/Switches/Modems/Printers

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: Routers/Switches/Modems/Printers	
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 router/switch/modem/printer until an image can be saved of the device's memory. SAVE an image of the configuration software and volatile memory (if possible and unless otherwise directed) for forensic analysis.
3.	REMOVE AND REPLACE the affected router/switch/modem/printer. Device replacement will preserve forensic evidence of the cyber incident for analysis as long as the device is connected to a power source and the device is not turned off.
4.	DO NOT REIMAGE any devices unless authorized by the ISSM. Reimaging the affected router/switch/modem/printer will destroy forensic evidence of the cyber incident. If a replacement router/switch/modem/printer is not available, REIMAGE the affected router/switch/modem/printer soft/firmware from a trusted, known good back-up source.
5.	VERIFY the latest vendor software/firmware patches are installed on the router/switch/modem/printer. INSTALL updates as required.
6.	UPDATE passwords on router/switch/modem/printer. UTILIZE robust passwords.
7.	SELECT the optional selectable IP range (if available) for the router/switch/modem instead of the default IP range.

Typical Equipment: Routers/Switches/Modems/Printers	
Reintegration	
8.	<p>Do NOT reconnect the router/switch/modem/printer to other devices in the network until each device in the network layer or sub-system has been recovered per these procedures.</p> <p>VERIFY that each device in the isolated layer or sub-system has been properly recovered. CONSULT the cyber incident records, the ISSM, or CPT to confirm that <i>Recovery</i> has been performed on these devices.</p>
9.	<p>When each device in the layer or sub-system has been recovered per these procedures, RECONNECT all of the devices in the layer or sub-system.</p> <p>DO NOT RECONNECT to the wider network at this time.</p>
10.	<p>VERIFY that the cyber incident artifacts have been eliminated using available <i>Detection</i> tools (IDS, Log Review, Netstat, Wireshark, etc).</p>
11.	<p>MONITOR the system for anomalous behavior.</p> <p>If anomalous behavior is evident, RETURN to the <i>Detection Procedures</i> (enclosure A) and/or <i>Mitigation Procedures</i> (enclosure B) of this ACI TTP as necessary.</p>
12.	<p>When the layer or sub-system is operating without evidence of the cyber incident and approval is given by the ISSM or CPT, RECONNECT the isolated layer or sub-system to the rest of the network.</p>
13.	<p>MONITOR the system for anomalous behavior.</p> <p>If anomalous behavior is evident, RETURN to the <i>Detection Procedures</i> (enclosure A) and/or <i>Mitigation Procedures</i> (enclosure B) of this ACI TTP as necessary.</p>
14.	SUBMIT all records of <i>Recovery</i> actions to the ISSM or CPT.
15.	RETURN to <i>Routine Monitoring</i> of the network.

C.3. Recover – RTU, MTU, and PLC

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: RTU/MTU/PLC	
Step	Recovery Procedure
1.	<ul style="list-style-type: none"> 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: <ol style="list-style-type: none"> 1. FMC baseline topology 2. Jump-Kit
2.	<p>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.</p> <p>MAINTAIN primary power (if possible) to the RTU/MTU/PLC until an image can be saved of the device's memory.</p> <p>SAVE an image of the configuration software and volatile memory (if possible and unless otherwise directed) for forensic analysis.</p>
3.	<p>REMOVE AND REPLACE the affected RTU/MTU/PLC. Device replacement will preserve forensic evidence of the cyber incident for analysis.</p>
4.	<p>DO NOT REIMAGE any devices unless authorized by the ISSM. Reimaging the affected RTU/MTU/PLC will destroy forensic evidence of the cyber incident.</p> <p>If a replacement RTU/MTU/PLC or modules are not available, REIMAGE the affected RTU/MTU/PLC software/firmware from a trusted, known good source.</p>
5.	<p>VERIFY the latest vendor software/firmware patches are installed on the RTU/MTU/PLC. INSTALL updates as required.</p>
6.	<p>UPDATE passwords on RTU/MTU/PLC. UTILIZE robust passwords.</p>
7.	<p>CONFIRM/UPDATE the RTU/MTU/PLC set points and configuration files.</p>
8.	<p>TEST the operation of the RTU/MTU/PLC and the endpoint device(s) while in local operating mode and while still isolated from the wider network (when operating conditions allow).</p>
Reintegration	
9.	<p>DO NOT RECONNECT the RTU/MTU/PLC to other network devices in the affected network until each device in the network layer or sub-system has been recovered per these procedures.</p>

Typical Equipment: RTU/MTU/PLC	
10.	VERIFY that each device in the isolated layer or sub-system has been properly recovered. CONSULT the cyber incident records, the ISSM, or CPT to confirm that <i>Recovery</i> has been performed on these devices.
11.	When each device in the sub-system or layer has been recovered, RECONNECT all of the devices in the sub-system or layer. DO NOT RECONNECT to the wider network at this time.
12.	VERIFY that the cyber incident artifacts have been eliminated using available <i>Detection</i> tools (IDS, Log Review, NMap, Netstat, Wireshark, etc).
13.	MONITOR the system for anomalous behavior. If anomalous behavior is evident, RETURN to the <i>Detection Procedures</i> (enclosure A) and/or <i>Mitigation Procedures</i> (enclosure B) of this ACI TTP as necessary.
14.	When the layer or sub-system is operating without evidence of the cyber incident, and approval is given by the ISSM or CPT, RECONNECT the isolated layer or sub-system to the rest of the network.
15.	MONITOR the system for anomalous behavior. If anomalous behavior is evident, RETURN to the <i>Detection Procedures</i> (enclosure A) and/or <i>Mitigation Procedures</i> (enclosure B) of this ACI TTP as necessary.
16.	SAVE an image of the new firmware/configuration hash.
17.	RETURN to <i>Routine Monitoring</i> of the network.
18.	SUBMIT all records of <i>Recovery</i> actions to the ISSM or CPT.

C.4. Recover – Intelligent Electronic Devices (IEDs)

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: IEDs; Protective Relay Controllers, Tap Changer Controllers, Circuit Breaker Controllers, Capacitor Bank Switches, Switch Re-closer Controllers, Voltage Regulators, Etc.	
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 IED until an image can be saved of the device's memory. SAVE an image of the configuration software and volatile memory (if possible) for forensic analysis.
3.	REMOVE AND REPLACE the affected IED. Device replacement will preserve forensic evidence of the cyber incident for analysis.
4.	DO NOT REIMAGE any devices unless authorized by the ISSM. Reimaging the affected IED will destroy forensic evidence of the cyber incident. If a replacement IED is not available, REIMAGE the affected IED from a trusted, known good source.
5.	VERIFY the latest vendor software/firmware patches are installed on the IED. INSTALL updates as required.
6.	UPDATE passwords on the IED. USE robust passwords.
7.	SELECT the optional selectable IP range instead of the default IP.
8.	CONFIRM/UPDATE the IED set points and configuration files as required.
9.	SAVE an image of the new firmware/configuration hash.
10.	TEST the operation of the IED and the endpoint device while in local operating mode and while still isolated from the wider network (when operating conditions allow).
Reintegration	
11.	DO NOT RECONNECT the IED to other network devices in the network until each device in the network layer or sub-system affected has been recovered per these procedures.

Typical Equipment: IEDs; Protective Relay Controllers, Tap Changer Controllers, Circuit Breaker Controllers, Capacitor Bank Switches, Switch Re-closer Controllers, Voltage Regulators, Etc.	
12.	VERIFY that each device in the isolated layer or sub-system has been properly recovered. CONSULT the cyber incident records, the ISSM, or CPT to confirm that <i>Recovery</i> has been performed on these devices.
13.	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.
14.	VERIFY that the cyber incident artifacts have been eliminated using available <i>Detection</i> tools (IDS, Log Review, NMap, Netstat, Wireshark, etc).
15.	MONITOR the system for anomalous behavior. If anomalous behavior is evident, RETURN to the <i>Detection Procedures</i> (enclosure A) and/or <i>Mitigation Procedures</i> (enclosure B) of this ACI TTP as necessary.
16.	When the layer or sub-system is operating without evidence of the cyber incident, and approval is given by the ISSM or CPT, RECONNECT the isolated layer or sub-system to the rest of the network.
17.	MONITOR the system for anomalous behavior. If anomalous behavior is evident, RETURN to the <i>Detection Procedures</i> (enclosure A) and/or <i>Mitigation Procedures</i> (enclosure B) of this ACI TTP as necessary.
18.	SAVE an image of the new firmware/configuration hash.
19.	SUBMIT all records of <i>Recovery</i> actions to the ISSM or CPT.
20.	RETURN to <i>Routine Monitoring</i> of the network.

C.5. Recover – Human-Machine Interface (HMI)

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: Human-Machine Interface (HMI)	
Step	Recovery Procedure
1.	<p>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.</p>
2.	<p>MAINTAIN primary power (if possible) to the HMI until an image can be saved of the device's memory.</p> <p>SAVE an image of the configuration software and volatile memory (if possible and unless otherwise directed) for forensic analysis.</p>
3.	REMOVE AND REPLACE the affected HMI. Device replacement will preserve forensic evidence of the cyber incident for analysis
4.	If a replacement HMI is not available, REMOVE AND REPLACE the hard drive (if installed) with a back-up drive containing software from a trusted, known good source.
5.	<p>DO NOT REIMAGE any devices unless authorized by the ISSM or CPT. Reimaging the affected HMI will destroy forensic evidence of the cyber incident.</p> <p>If a replacement HMI or hard drive is not available, REIMAGE the affected HMI from a trusted, known good back-up source.</p>
6.	<p>Rootkit infections/detections will require REFLASHING of the BIOS on the server/workstation. An example of generic BIOS reflash procedure follows. Check your vendor documentation for specific instructions for your device. Before you REFLASH the BIOS:</p> <ol style="list-style-type: none"> DISABLE BIOS Flash Protection in the BIOS setup. VERIFY the BIOS version update is the correct BIOS for your machine. Do not interrupt the BIOS when updating; improper BIOS flashing will result in system malfunctions. When the BIOS REFLASH is complete, ENABLE BIOS Flash Protection in the BIOS setup menu.

Typical Equipment: Human-Machine Interface (HMI)	
7.	VERIFY the latest vendor software/firmware patches are installed on the HMI. INSTALL updates as required.
8.	UPDATE passwords on HMI. UTILIZE robust passwords.
9.	VERIFY that system configurations are correctly displayed on the HMI.
10.	UPDATE the antivirus software (if installed) with the latest update, and INITIATE a full system scan.
Reintegration	
11.	DO NOT RECONNECT the HMI to other network devices in the network until each device in the network layer or sub-system affected has been recovered per these procedures.
12.	VERIFY that each device in the isolated layer or sub-system has been properly recovered. Consult the cyber incident records, the ISSM, or CPT to confirm that Recovery has been performed on these devices. <ul style="list-style-type: none"> a. RECONNECT the device or sub-system. b. DO NOT RECONNECT to the wider network at this time.
13.	VERIFY that the cyber incident artifacts have been eliminated using available <i>Detection</i> tools (IDS, Log Review, NMap, Netstat, Wireshark, etc.).
14.	MONITOR the process being controlled for anomalous behavior. If anomalous behavior is evident, RETURN to the <i>Detection Procedures</i> (enclosure A) and/or <i>Mitigation Procedures</i> (enclosure B) of this ACI TTP as necessary.
15.	VERIFY that changes in system indications are accurately indicating on the HMI, and the HMI has proper control over the system.
16.	When the layer or sub-system is operating without evidence of the cyber incident and approval is given by the ISSM or CPT, RECONNECT the isolated layer or sub-system to the rest of the network.
17.	MONITOR the system for anomalous behavior. If anomalous behavior is evident, RETURN to the <i>Detection Procedures</i> (enclosure A) and/or <i>Mitigation Procedures</i> (enclosure B) of this ACI TTP as necessary.
18.	SUBMIT all records of <i>Recovery</i> actions to the ISSM or CPT.
19.	RETURN to <i>Routine Monitoring</i> of the network.

C.6. Recover – Firewalls

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: Firewalls	
Step	Recovery Procedure
1.	<p>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.</p>
2.	<p>MAINTAIN primary power to the firewall until efforts can be made to SAVE the contents of the device's volatile memory. This will preserve forensic evidence of the cyber incident for analysis.</p> <p>SAVE a copy of the IOS image and a copy of the startup and running configuration files (if possible and unless otherwise directed) for forensic analysis.</p>
3.	<p>If the firewall is a physical hardware device, REMOVE AND REPLACE the affected firewall if a replacement is available. Device replacement will preserve forensic evidence of the cyber incident for analysis.</p>
4.	<p>DO NOT REIMAGE any devices unless authorized by the ISSM or CPT. Reloading an image to the affected firewall will destroy forensic evidence of the cyber incident; when possible, save the image for forensic analysis.</p> <p>If a replacement firewall is not available, ensure that startup configuration, running configuration, and IOS image are backed up. Then REIMAGE the affected firewall from a trusted, known good back-up source.</p>
5.	<p>If the firewall is software only, REMOVE AND REPLACE the hard drive containing the firewall software with a known, good back up, or if not available, REIMAGE the affected drive/firewall from a trusted, known good back-up source.</p> <p>DO NOT REIMAGE any components unless authorized by the ISSM or CPT. Reimaging the affected firewall will destroy forensic evidence of the cyber incident.</p>

Typical Equipment: Firewalls	
6.	VERIFY the Firewall Access Control List configuration and ensure that the device is setup to allow only authorized network traffic. For example: ASA# show access-list.
Reintegration	
7.	DO NOT RECONNECT the firewall to other devices in the network until each device in the network layer or sub-system affected has been recovered per these procedures.
8.	VERIFY that each device in the isolated layer or sub-system has been properly recovered. Consult the cyber incident records, the ISSM, or CPT to confirm that <i>Recovery</i> has been performed on these devices. <ul style="list-style-type: none"> a. RECONNECT the device or sub-system. b. DO NOT reconnect to the wider network at this time.
9.	VERIFY that the cyber incident artifacts have been eliminated using available <i>Detection</i> tools (IDS, Log Review, NMap, Netstat, Wireshark, etc).
10.	MONITOR the system for anomalous behavior. If anomalous behavior is evident, RETURN to the <i>Detection Procedures</i> (enclosure A) and/or <i>Mitigation Procedures</i> (enclosure B) of this ACI TTP as necessary.
11.	When the layer or sub-system is operating without evidence of the cyber incident, and approval is given by the ISSM or CPT, RECONNECT the isolated layer or sub-system to the rest of the network.
12.	MONITOR the system for anomalous behavior. If anomalous behavior is evident, RETURN to the <i>Detection Procedures</i> (enclosure A) and/or <i>Mitigation Procedures</i> (enclosure B) of this ACI TTP as necessary.
13.	SUBMIT all records of <i>Recovery</i> actions to the ISSM or CPT.
14.	RETURN to <i>Routine Monitoring</i> of the network.

C.7. Recover – Media Converters (Serial/Fiber Converter)

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: Media Converters (Serial to Fiber, Serial to Ethernet)	
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.	REMOVE AND REPLACE the affected converter.
3.	If the converter contains firmware and a replacement is not available, REFLASH the firmware from a trusted source.
Reintegration	
5.	DO NOT reconnect devices or network layers until each component has been functionally tested and all attributes of the cyber incident have been eliminated.
6.	VERIFY that each device in the isolated layer or sub-system has been properly recovered. CONSULT the cyber incident records, the ISSM, or CPT to confirm that Recovery has been performed on these devices. <ol style="list-style-type: none"> RECONNECT the device or sub-system. DO NOT reconnect to the wider network at this time.
7.	VERIFY that the cyber incident artifacts have been eliminated using available <i>Detection</i> tools (IDS, Log Review, NMap, Netstat, Wireshark, etc).
8.	MONITOR the system for anomalous behavior. If anomalous behavior is evident, RETURN to the <i>Detection Procedures</i> (enclosure A) and/or <i>Mitigation Procedures</i> (enclosure B) of this ACI TTP as necessary.
9.	When the layer or sub-system is operating without evidence of the cyber incident, and approval is given by the ISSM or CPT, RECONNECT the isolated layer or sub-system to the rest of the network.

Typical Equipment: Media Converters (Serial to Fiber, Serial to Ethernet)	
10.	MONITOR the system for anomalous behavior. If anomalous behavior is evident, RETURN to the <i>Detection Procedures</i> (enclosure A) and/or <i>Mitigation Procedures</i> (enclosure B) of this ACI TTP as necessary.
11.	SUBMIT all records of <i>Recovery</i> actions to the ISSM or CPT.
12.	RETURN to <i>Routine Monitoring</i> of the network.

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	
Step	Routine Monitoring Procedure
1.	<p>COMPARE expected normal ICS activity to observed ICS activity, and search for differences (which are also called anomalies throughout this TTP).</p> <p>a. If an anomaly is found, LOCATE anomaly (or the closest description of the anomaly) in Enclosure A: Detection Procedures, A.1.1 <i>Event Diagnostics Table</i>. FOLLOW the instructions in the Event Diagnostics Table. The instructions will lead to:</p> <p>(1) An evaluation of the anomaly.</p>

Routine Monitoring: Overview	
	<p>(2) A ranking of the anomaly's Severity Level.</p> <p>(3) A list of next steps.</p> <p>b. Once the anomaly event has been resolved, ICS operators should RETURN to <i>Routine Monitoring</i> activities.</p> <p>c. If the ICS activity is normal, <i>Routine Monitoring</i> should continue as prescribed in the command's ICS <i>Routine Monitoring</i> schedule.</p>
2.	The following steps (instructions) provide details for the use of this enclosure.
3.	<p>Establish INFOCON: CONTACT the ISSM and obtain the INFOCON status.</p> <p>a. If the INFORCON status is normal, the periodicity of <i>Routine Monitoring</i> is accomplished during normal operations, using normal monitoring checks.</p> <p>b. If the INFOCON is elevated, integrate checks marked "2nd Stage Monitoring" into <i>Routine Monitoring Schedule</i>.</p>
4.	<p>Develop Routine Monitoring Schedule: IT (or ICS) personnel conduct these checks. If IT personnel are not assigned to the ICS, work with the command Network Engineers and ISSM to integrate event checking for ICS. The <i>Routine Monitoring</i> tasks are divided into the following sections:</p> <p>a. <i>Security Events</i>: events occurring on Intrusion Detection Systems (IDS), firewalls, virus checkers, and Syslogs, or Security Information and Event Management (SIEMs) if available.</p> <p>b. <i>Computer Assets</i>: servers, workstations, to include HMI, Historians, OPC, and engineering workstations. Checks normally conducted by IT or ICS operators.</p> <p>c. <i>Network Flow</i>: IT operators generally check network data flows.</p> <p>d. <i>Synchronicity Check</i>: HMI, OPC, engineering workstation checks against controller status. ICS operator personnel conduct these checks.</p> <p>e. <i>Synchronicity Check</i>: controllers to endpoint device status checks conducted by ICS operators.</p> <p>f. <i>Historian</i>: status check for abnormal activities. Checks conducted by either IT or ICS operators.</p>
5.	<p>Integrating Routine Monitoring Into Daily Schedule: <i>Routine Monitoring</i> Procedures are designed to integrate with daily routines found in an ICS environment.</p> <p>a. Map each <i>Routine Monitoring</i> task to the individuals most likely to perform the check.</p> <p>b. Extract <i>Routine Monitoring</i> instructions and tables (make copies as needed) and integrate these with daily ICS procedures. These procedures can include safety monitoring procedures, meter recording procedures, equipment monitoring, "tuning loops," and operations checks.</p> <p>c. EXTRACT the <i>Routine Monitoring Schedule</i> (table D-1 below), and annotate it with the area being monitored, the individual(s) conducting the check, days</p>

Routine Monitoring: Overview	
	<p>checks should be conducted, and the time they should be conducted. STORE Routine Monitoring Schedule with management documents for quick referral.</p> <p>d. REVIEW Routine Monitoring Procedures with individuals conducting checks, and ensure procedures are understood.</p> <p>e. EXECUTE Routine Monitoring Schedule.</p> <p>f. If the command is operating at an elevated INFOCON level, in addition to executing the <i>Routine Monitoring Schedule</i>, EXECUTE the <i>2nd Stage Monitoring</i> checks as well.</p>

ICS Cyber Security Routine Monitoring Schedule			
Monitoring Area	Operator	Monitoring Days	Monitoring Times
Security Events and IDS			
Security Events and Firewall Log Check			
Network Flow			
HMI Layer 2			
HMI Layer 1			
OPC Server			
Engineering Workstation			
Primary Historian			
Secondary Historian			
Synchronicity Check Layer 2-1			
Synchronicity Check Layer 1-0			
Computer Assets			

NOTE: Monitoring area includes suggested assets to monitor. If your installation does not have these devices, or they are located in a different layer, modify table to map to your ICS.

Table D-1: Routine Monitoring Schedule

D.3. Routine Monitoring: Security Events and IDS Alert Check

Routine Monitoring: Security Events and IDS Alert Check	
Step	IDS Alert Check Procedure
1.	MAKE a copy of the <i>FMC Data Flow Table</i> and the <i>FMC Topology Diagram</i> and RETURN the originals to the <i>FMC Baseline Documents</i> binder.
2.	ACCESS the IDS console (this may be different for each command) that monitors network traffic in ICS Layers 1 and 2.
3.	<p>REVIEW IDS alerts for events listed below. Refer to the <i>FMC Data Flow Table</i> for approved and normal IP/MAC to IP/MAC communications.</p> <ul style="list-style-type: none"> a. Unexpected patch updates. b. Stop commands to controllers coming from unapproved IP/MAC addresses. c. Machines or intelligent field devices connecting to unknown, or unapproved external IP addresses. d. Inbound Telnet, FTP, TFTP, Modbus, DNP3 (or other ICS field controller protocol traffic). e. Inbound or outbound HTTP or HTTPS coming from or going to unknown or unapproved IP/MAC address. f. Unexpected field controller connection to an external IP address. g. Unusual lateral connections between ICS assets. h. Any function codes or commands directed at field controllers and not coming from approved IP/MAC addresses.
4.	If alerts described in item 3 are found, GO TO Enclosure A: Detection Procedures, A.1.1 <i>Event Diagnostics Table</i> . Locate Event on <i>Event Diagnostics Table</i> and execute the procedures described in the table.
5.	If no alerts are found, CONTINUE Routine Monitoring.
2nd Stage Monitoring	
6.	<p>CHECK if IDS is functioning correctly. To accomplish this, look for the following symptoms:</p> <ul style="list-style-type: none"> a. IDS has not issued alerts for an unusual amount of time (IDS often issues alerts that are deemed “false positives” and are often known by personnel). b. Keyboard is locking up. c. IDS spontaneously reboots. d. Display screen has changed for no apparent reason. e. Any symptom indicating IDS is malfunctioning.

Routine Monitoring: Security Events and IDS Alert Check	
7.	If anomalous events are found, GO TO Enclosure A: Detection Procedures, A.1.1 <i>Event Diagnostics Table</i> , and EXECUTE the procedures described in the table.
8.	If no anomalous events are found, RETURN to <i>Routine Monitoring with 2nd Stage Monitoring</i> .

D.4. Routine Monitoring: Security Events and Firewall Log Check

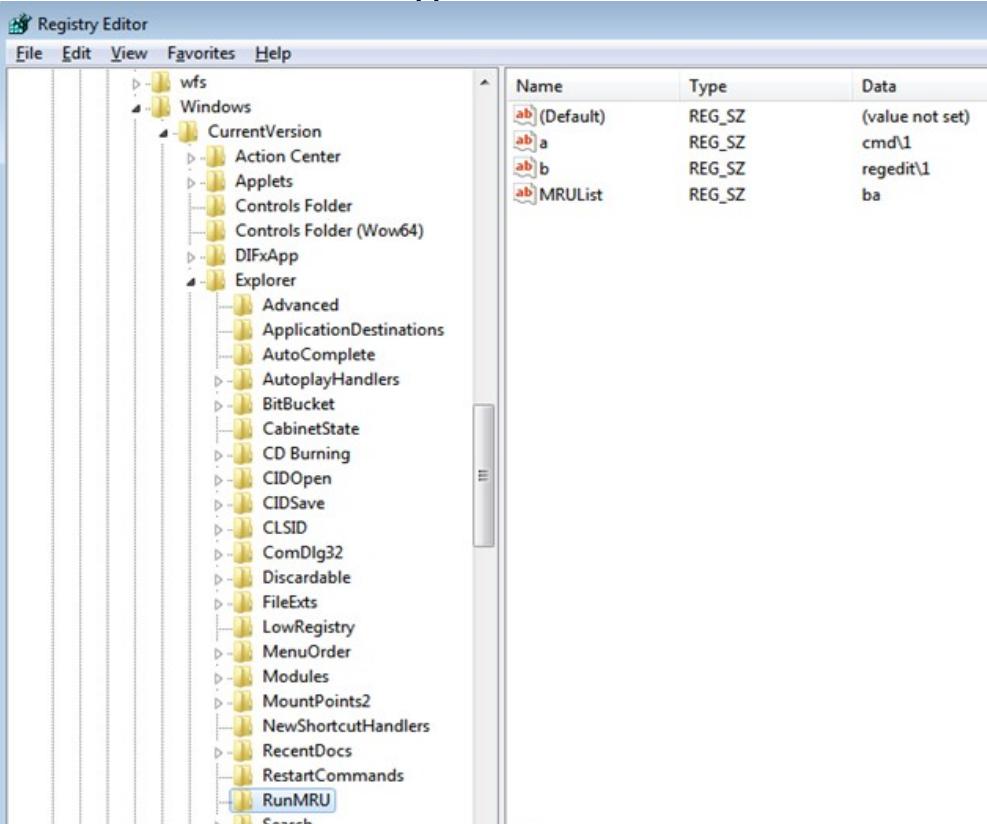
Routine Monitoring: Security Events and Firewall Log Check	
Step	Firewall Log Check Procedure
1.	MAKE a copy of the <i>FMC Data Flow Diagram</i> and the <i>FMC Topology Diagram</i> , and RETURN the originals to the <i>FMC Baseline Documents</i> binder.
2.	ACCESS the firewall console (this may be different for each command) that monitors network traffic in ICS Layers 1 and 2.
3.	<p>REVIEW firewall log for events listed below. Refer to the <i>FMC Data Flow Diagram</i> for approved and normal IP/MAC to IP/MAC communications.</p> <ul style="list-style-type: none"> a. Unexpected patch updates. b. Stop commands to controllers coming from unapproved IP/MAC addresses. c. Machines or intelligent field devices connecting to unknown or unapproved external IP addresses. d. Inbound Telnet, FTP, TFTP, Modbus, DNP3 (or other ICS field controller protocol traffic). e. Inbound or outbound HTTP or HTTPS coming from or going to unknown or unapproved IP/MAC address. f. Unexpected field controller connection to an external IP address. g. Unusual lateral connections between ICS assets. h. Any function codes or commands directed at field controllers and not coming from approved IP/MAC addresses.
4.	<p>If events as described in item 3 are found, GO TO Enclosure A: Detection Procedures, A.1.1 <i>Event Diagnostics Table</i>. Locate Event on <i>Event Diagnostics Table</i> and EXECUTE the procedures described in the table.</p> <p>If no alerts are found, continue <i>Routine Monitoring</i> or if INFOCON level is elevated, CONTINUE with step 5.</p>
2nd Stage Monitoring	
5.	<p>CHECK if firewall is functioning correctly. To accomplish this, LOOK for the following symptoms:</p> <ul style="list-style-type: none"> a. Firewall does not log any information. b. Keyboard is locked up. c. Firewall spontaneously reboots. d. Display screen changes for no apparent reason. e. Any symptom that indicates the firewall is malfunctioning.
6.	If anomalous events are found (as described in item 5), GO TO A.3.3.10 <i>Firewall Integrity Check</i> , and execute the procedures.
7.	If no anomalous events are found, RETURN to <i>Routine Monitoring</i> .

D.5. Routine Monitoring: Computer Assets

Routine Monitoring: Computer Assets	
Step	Computer Assets Procedures
1.	MAKE a copy of the <i>FMC Data Flow Diagram</i> , <i>User Account Table</i> , and the <i>FMC Topology Diagram</i> , and RETURN the originals to the <i>FMC Baseline Documents</i> binder.
2.	LOG on to asset, and run as “administrator”.
3.a.	<p>DISPLAY Security Log - Windows 7:</p> <ol style="list-style-type: none"> To open Event Viewer, click Start, click Control Panel, click System and Maintenance, double-click Administrative Tools, and then double-click Event Viewer. OPEN Event Viewer. In the console tree, open Global Logs, and then click Security. The results pane lists individual security events. If the event volume is high, it may be helpful to Filter the Security Log for: Critical, Warning, and Error events.
3.b.	<p>DISPLAY Security Log - Windows 10:</p> <ol style="list-style-type: none"> To open Event Viewer, right-click Start, click Control Panel, click System and Security, under Administrative Tools click View event logs. OPEN Event Viewer. In the console tree, open Windows Logs, and then click Security. The results pane lists individual security events. If the event volume is high, right-click on Security, select Filter Current Log, then select: Critical, Warning, and Error.
4.	<p>REVIEW Security Logs since last <i>Routine Monitoring</i> check for the following user actions:</p> <ol style="list-style-type: none"> Unauthorized user logging in. Rapid and/or continuous log-ins/log-outs. Users logging into accounts outside of normal working hours and for no apparent reason. Numerous failed log-in attempts found in logs on administrator accounts or other user accounts. User accounts attempting to escalate account privileges or access areas or assets not required by their jobs. Logs that have been erased or appear altered (look for missing days or times).

Routine Monitoring: Computer Assets	
<p>5. If events as described in item 4 are found, GO TO Enclosure A: Detection Procedures, A.1.1 <i>Event Diagnostics Table</i>. Locate Event on <i>Event Diagnostics Table</i>, and execute the procedures described in the table.</p> <p>If no alerts are found, CONTINUE to next <i>Routine Monitoring</i> check.</p>	
<p>6. In Windows, open a command prompt (for detailed instructions, see Appendix D: References, NSA document, <i>Position Zero</i>). Execute the following command:</p> <pre>c:\> netstat -ano more</pre>	
<p>7. The netstat command in step 6 will display information about connections to and from the asset you are monitoring. Using the <i>FMC Data Flow Diagram</i>, LOCATE the asset you are monitoring.</p> <p>COMPARE the expected connections in the table to the connections you displayed using the netstat command. Or, compare to baseline netstat if available.</p>	
<p>8. If the asset is connecting to devices not found in the table, GO TO Enclosure A: Detection Procedures, A.1.1 <i>Event Diagnostics Table</i>. Locate Event on <i>Event Diagnostics Table</i>, and execute the procedures described in the table.</p> <p>If no alerts are found, CONTINUE Routine Monitoring, or if INFOCON level is elevated, continue with step 10.</p>	
2nd Stage Monitoring- Unauthorized Processes Check Procedure	
<p>9. INSERT the Baseline CD-r or DVD-r (media) into the drive of the device you are monitoring.</p> <ul style="list-style-type: none"> a. USING the Windows directory display feature, display the files on the media. b. LOCATE the files associated with the asset you are inspecting (should be labeled by asset name). 	
<p>10. OPEN a command line from the Windows desktop.</p>	
<p>11. EXECUTE the following command to compare authorized processes documented in the baseline to the current processes executing on the asset:</p> <pre>c:\> tasklist /m /fo list > (asset name)-(date)-Proc-dll.txt</pre> <p>Example: c:\> tasklist /m /fo list > HMI1-03232015-Proc-dll.txt</p> <p>EXECUTE the next command:</p> <pre>C:\> FINDSTR /VIXG: (media drive name):(asset name)-Proc-dll.txt (the name of the file you created in the preceding step) > comp-proc-dll.txt</pre> <p>Example: c:\> FINDSTR /VIXG: e:\HMI1-Proc-dll.txt HMI1-03232015-Proc-dll.txt >comp-proc-dll.txt</p> <p>For more detailed methods to detect unauthorized processes, see Appendix E, item EE.7</p>	
<p>12. Display the file you just created (comp-proc-dll.txt) using Notepad (see Appendix D:</p>	

Routine Monitoring: Computer Assets	
	References, NSA document, <i>Position Zero</i> , for instructions if needed).
13.	IDENTIFY processes and DLLs that do not correspond to regular process files (refer to Windows documentation if needed).
14.	If irregular processes are found, GO TO Enclosure A: Detection Procedures, A.1.1 <i>Event Diagnostics Table</i> , and execute the procedures described in the table (e.g. section A.2.3). If no irregular processes are found, CONTINUE Routine Monitoring .
Antivirus Services Check Procedure (MS Windows Only)	
15.	DETERMINE if antivirus software is running properly. For centrally managed antivirus products generate (or request) the appropriate reports, then continue to step 18. For unmanaged systems continue to step 16.
16.	In Control Panel, DETERMINE the status of the services associated with antivirus software and GO TO step 18. To run these checks from the command line, proceed to step 17.
17.	USE the "sc query" and "sc GetKeyName" commands to get a list of the relevant antivirus services and query their status. (If needed, see Appendix E: Technical Supplement, section EE.5 "Health" Checks for Antivirus, Host Based/EndPoint Protection Software).
18.	If irregular status of a service is found: a. DOCUMENT the details in the Security Log. b. DOCUMENT the Severity Level of High (3) . c. GO TO section A.2.29 Action Step .
19.	If no anomaly was found: a. DOCUMENT the Severity Level as None (0) . b. CONTINUE Routine Monitoring .
Antivirus DAT/Definition Check Procedure (MS Windows Only)	
20.	DETERMINE if antivirus DAT/definitions are current. For centrally managed antivirus products generate (or request) the appropriate reports and then continue to step 23. For unmanaged systems continue to step 21 to evaluate from the local GUI, or continue to step 22 to evaluate from the local command line.
21.	From the Windows system tray, RIGHT-CLICK the antivirus icon and select the appropriate item to get product details. NOTE the definition/DAT dates and SKIP to step 23.
22	OBTAIN the version of the antivirus DAT/definitions via command line registry query. e.g. reg query HKLM\Software\Wow6432Node\McAfee\AVEngine reg query "HKLM\SOFTWARE\Symantec\Symantec Endpoint Protection\CurrentVersion\SharedDefs" (If needed, see Appendix E: Technical Supplement, section EE.5 "Health" Checks for

Routine Monitoring: Computer Assets																
	Antivirus, Host Based/EndPoint Protection Software).															
23.	Compare the date of the last antivirus DAT/definition update to the current date.															
24.	If DAT/definitions are older than mandated by DoD configuration policy: <ol style="list-style-type: none"> DOCUMENT the details in the Security Log. DOCUMENT the Severity Level of High (3). GO TO section A.2.29 Action Step. 															
25.	If DAT/definitions are current in accordance with DoD configuration policy: <ol style="list-style-type: none"> DOCUMENT the Severity Level as None (0). CONTINUE Routine Monitoring. 															
Command Shell Detection																
26.	Detect unexpected spawning of shell commands. The “Run” key history, found in the Windows Registry (regedit), may indicate if cmd was run. a. Navigate to the following key and review for unexpected activity: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Run MRU															
For additional methods, see Appendix E, item EE.6  <table border="1"> <thead> <tr> <th>Name</th> <th>Type</th> <th>Data</th> </tr> </thead> <tbody> <tr> <td>(Default)</td> <td>REG_SZ</td> <td>(value not set)</td> </tr> <tr> <td>a</td> <td>REG_SZ</td> <td>cmd\1</td> </tr> <tr> <td>b</td> <td>REG_SZ</td> <td>regedit\1</td> </tr> <tr> <td>MRUList</td> <td>REG_SZ</td> <td>ba</td> </tr> </tbody> </table>		Name	Type	Data	(Default)	REG_SZ	(value not set)	a	REG_SZ	cmd\1	b	REG_SZ	regedit\1	MRUList	REG_SZ	ba
Name	Type	Data														
(Default)	REG_SZ	(value not set)														
a	REG_SZ	cmd\1														
b	REG_SZ	regedit\1														
MRUList	REG_SZ	ba														

Detect Malware manipulation of state for legitimate processes	
27.	<p>Process kill/start: event logs usually only show graceful service/process stops. Since there is usually nothing logged for an ungraceful kill, instead try detecting the subsequent process start.</p> <p>Alternately, look for time anomalies:</p> <ul style="list-style-type: none">- Short run time: Review processes that should be "long running" yet have recent start times (list processes by shortest runtime, look in to application processes with shortest runtime)- Missing time: missing entries in application logs, missing heartbeats <p>For detailed methods, see Appendix E, item EE.8</p>

Detect unusual/unauthorized attachment and removal to processes	
<p>28. First, Identify your critical applications and their associated processes. Next, Detect process injection (e.g. DLL injection) attempts/attacks against these critical application executables/DLLs.</p> <p>Numerous methods of process injection exist on Windows, including: modifying the Registry, creating remote threads, hooking APIs, and DLL pre-loading. Some detection methods may require either 3rd party tools or specialized expertise, however some methods can be detected simply and are listed as follows:</p> <p>Method 1 Search Windows Registry (regedit) service keys for unexpected DLL loads. Note however that service keys are voluminous and most matches are likely to be legitimate. Focus on critical application services. A baseline comparison will help to identify suspicious DLL loads. <code>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\</code></p> <p>Method 2 Search Windows Registry (regedit) run keys for unexpected DLL loads. Or, as an administrator, use Microsoft SysInternals utility "Autoruns" and review the "known DLLs" tab and "services" tab for dlls and exes.</p> <p>Method 3 Search for unexpected DLLs in user directory. Also search for unexpected DLLs outside of the Windows and "Program Files" directories.</p> <p>Method 4 Periodically enumerate the DLL name list and compare against a baseline run. See section EE.7 subsection D, listdlls item for details and Enclosure E FMC Baseline, step E.6, section b.2.c for baseline information.</p> <p>Method 5 Use Windows tasklist (with switches) to identify unknown/unexpected DLLs attached to the legitimate application process. <code>tasklist /m /fi "imagename eq [executable]"</code></p> <p>e.g.</p> <pre>C:\>tasklist /m /fi "imagename eq cmd.exe" Image Name PID Modules ===== cmd.exe 5892 ntdll.dll, kernel32.dll, KERNELBASE.dll, SYSFER.DLL, msrvct.dll, WINBRAND.dll, USER32.dll, GDI32.dll, LPK.dll, USP10.dll, IMM32.DLL, MSCTF.dll, apphelp.dll</pre> <p>For additional details and methods, see Appendix E, item EE.9</p>	

Detect malware overwrite of an existing application or Windows service image path	
29.	<p>Detect evidence of malware persistence in the Windows Registry.</p> <p>Review information on system and application services and their full image paths from the following Windows registry section to detect evidence of malicious modification of image paths (e.g. to point to a malware binary).</p> <pre>HKLM\SYSTEM\CurrentControlSet\Services\<legitimate_service_names>\<ImagePath></pre> <p>To output all services' image path data from the registry, run the following query:</p> <pre>reg query HKLM\SYSTEM\CurrentControlSet\Services /fImagePath /s /t REG_EXPAND_SZ >> service-image-paths.txt</pre> <p>Compare the output to the baseline performed in Enclosure E. FMC Baseline, section E.6, subsection b.2.d Capture Services.</p> <p>If time constrained, review specific, targeted services and their full image path(s) against the baseline.</p> <p>e.g. To check image path to a single service:</p> <pre>C:\>reg query HKLM\SYSTEM\CurrentControlSet\Services /f \SystemRoot\system32\drivers\1394ohci.sys /s /t REG_EXPAND_SZ</pre> <pre>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\1394ohci ImagePath REG_EXPAND_SZ \SystemRoot\system32\drivers\1394ohci.sys</pre> <pre>End of search: 2 match(es) found.</pre> <p>check service to image path:</p> <pre>C:\>reg query HKLM\SYSTEM\CurrentControlSet\Services /f 1394ohci /s /t REG_EXPAND_SZ</pre> <pre>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\1394ohci ImagePath REG_EXPAND_SZ \SystemRoot\system32\drivers\1394ohci.sys</pre> <pre>End of search: 2 match(es) found.</pre> <p>For additional methods, see Appendix E, item EE.10</p>

Detect Malware manipulation of connected serial ports and devices	
30.	<p>Identify relevant processes/applications that use serial ports and check status:</p> <p>a. Open the command prompt and run the mode command. Note: this needs to be compared to a baseline reading (see Enclosure E FMC Baseline, step E.6, section b.2.h).</p> <p>e.g. C:\>mode com1</p> <pre>Status for device COM1: ----- Baud: 1200 Parity: None Data Bits: 7 Stop Bits: 1 Timeout: OFF XON/XOFF: OFF CTS handshaking: OFF DSR handshaking: OFF DSR sensitivity: OFF DTR circuit: ON RTS circuit: ON</pre> <p>Check device status: Device Status: MODE [device] [/STATUS]</p> <p>Note: To see mode command parameters run mode /?:</p> <p>e.g. C:\>mode /? Configures system devices.</p> <pre>Serial port: MODE COMM[:] [BAUD=b] [PARITY=p] [DATA=d] [STOP=s] [to=on off] [xon=on off] [odsr=on off] [octs=on off] [dtr=on off hs] [rts=on off hs tg] [idsr=on off] Device Status: MODE [device] [/STATUS] Redirect printing: MODE LPTn[:]=COMm[:] Select code page: MODE CON[:] CP SELECT=yyy Code page status: MODE CON[:] CP [/STATUS]</pre> <p>For additional methods, see Appendix E, item EE.11</p>

Detect unexpected changes to local/host firewall	
31.	<p>Review unexpected changes to local/host firewall rules, unexpected additions of trusted objects in local/host firewall, and firewall status.</p> <p>Monitor for the following Windows log EventIDs (Note: different versions of Windows may use different event ID numbers, be sure to use the correct version of event IDs.)</p> <p>2032 - Firewall Rule Processing - Windows Firewall has been reset to its default configuration.</p> <p>2033 - Firewall Rule Processing - All rules have been deleted from the Windows Firewall configuration on this computer.</p> <p>4688 - A new process has been created (this is not specifically Firewall related but it may occur as a result of a malware's procedures to affect the firewall).</p> <p>4956 - Firewall Rule Processing - Windows Firewall has changed the active profile.</p> <p>5024 - The Windows Firewall Service has been started</p> <p>5025 - The Windows Firewall Service has been stopped</p> <p>5030 - The Windows Firewall Service failed to start</p> <p>5034 - The Windows Firewall Driver has been stopped</p> <p>5035 - The Windows Firewall Driver failed to start</p> <p>5152, 5157, 5159 - Windows firewall is turned off</p> <p>5154 - The Windows Filtering Platform has permitted an application or service to listen on a port for incoming connections</p> <p>5158 - The Windows Filtering Platform has permitted a bind to a local port</p> <p>5050 - An attempt to programmatically disable the Windows Firewall...</p> <p>6400 - An attempt to programmatically disable the Windows Firewall...</p> <p>For Windows Firewall with Advanced Security - Enable advanced firewall logging: https://technet.microsoft.com/en-us/library/82164e05-3abe-428a-8b3d-7043462070e4</p> <p>Note: This activity logs to a file (not Windows event log).</p> <p>Firewall event log settings:</p> <p>“Firewall”. This log maintains events that relate to the configuration of Windows Firewall. For example, when a rule is added, removed, or modified, or when a network interface changes its profile, an event is added here.</p> <p>“FirewallVerbose”. This log maintains events that relate to the operational state of the firewall. For example, when a firewall rule becomes active, or when the settings of a profile are changed, an event is added here. This log is disabled by default. To enable this log, right-click FirewallVerbose, and then click Enable Log.</p>

D.6. Routine Monitoring: Network Data Flow

Routine Monitoring: Network Data Flow	
Step	Network Data Flow Procedure
1.	<ul style="list-style-type: none"> • Functional Area: IT or ICS • What you need to perform this procedure: <ol style="list-style-type: none"> 1. From the <i>FMC Baseline Documents</i> binder, extract <i>FMC Data Flow Diagram</i> and <i>Enclave Entry Points Table</i> for the assets being monitored 2. From the <i>FMC Baseline Documents</i> binder, extract <i>FMC Topology Diagram</i>
2.	<p>Beginning with your <i>Enclave Entry Points</i>, using the methodology your command has directed, OPEN console to the data flow capture tool for the first device at the Enclave Entry Point, and REVIEW network traffic. Comparing the network traffic to the authorized connections listed in the <i>Enclave Entry Points Table</i>, check for:</p> <ol style="list-style-type: none"> a. Undocumented IP addresses. b. Ports, protocols, and services. c. Anomalous traffic. Anomalous traffic can include (but is not limited to): <ol style="list-style-type: none"> (1) Network traffic appears blocked. (2) Unusually high network traffic or heavy traffic, particularly at the Enclave Entry Points. (3) Peripheral device or other network devices exhibiting unusual communication behaviors. (4) IP address seen originating from two or more distinct MAC addresses.
3.	If anomalous traffic is found in step 2, GO TO Enclosure A: Detection Procedures, A.1.1 <i>Event Diagnostics Table</i> . Locate Event on <i>Event Diagnostics Table</i> , and EXECUTE the procedures described in the table.
4.	REPEAT step 2 for each device listed in the <i>Enclave Entry Points</i> and <i>FMC Data Flow Table</i> .
5.	If no anomalous traffic is found, RETURN to <i>Routine Monitoring</i> with <i>2nd Stage Monitoring</i> actions.

D.7. Routine Monitoring: Synchronicity Check

Routine Monitoring: Synchronicity Check	
Step	Recovery Procedure
1.	<p>As field technicians validate field controllers, the HMI operator should contact Field Technician:</p> <p>VALIDATE that HMI ladder logic, configurations, and set points on HMI are synchronized with field controller.</p>
2.	<p>If unexpected changes are found, DETERMINE if these changes were authorized.</p> <p>If changes were not authorized, CHECK for a cyber event by going to Enclosure A: Detection Procedures, A.1.1 <i>Event Diagnostics Table</i>.</p> <ol style="list-style-type: none"> LOCATE the event that corresponds to the condition you have found. EXECUTE the actions listed in the Event Diagnostics Table.

This page intentionally left blank.

ENCLOSURE E: FULLY MISSION-CAPABLE (FMC) BASELINE

E.1. FMC Baseline Introduction

- a. **Description.** The FMC baseline consists of documentation that characterizes the ICS system.
- b. **Key Components**
 - (1) Topology diagram
 - (2) Enclave entry points
 - (3) User accounts
 - (4) Server/workstation documentation
 - (5) Network documentation

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).

E.3. FMC Baseline Procedures

The procedures for establishing an FMC Baseline involve the following:

- (1) Produce ICS Topology Diagram
- (2) Document network traffic entering and exiting the ICS in *Enclave Entry Point Chart* on page E-4
- (3) Document server/workstation user accounts; normal tasks and processes; connecting devices with ports, protocols, and services
- (4) Document normal network traffic

FMC Baseline:
<ul style="list-style-type: none"> • Functional Area: IT or ICS • What you need to perform this procedure: <ol style="list-style-type: none"> 1. One to five formatted <i>Write Once–Read Many</i> CD or DVD (CD-r, or DVD-r) 2. Laptop with Internet access (for downloads) 3. If available, network mapping tool for ICS 4. Plant documentation listing devices and their locations 5. A binder with label: <i>FMC Baseline Documents</i>

E.4. FMC Baseline Instructions

The ICS Topology Diagram describes which devices are located at which locations and how they connect. Generating an ICS Topology Diagram is accomplished using automated tools specifically designed for ICS in conjunction with manual “walk through” or simply using a manual “walk through” and inventory information or schematics if automated tools are not available.

a. Capture Assets

If you are using a network scanner, such as NMap (using SCADA script) or Nessus (with SCADA Plugin) or another tool that can provide an enumeration of live hosts on SCADA, scan your network to identify live assets.

- (1) Most scanning tools do not capture the location of devices that are not active. These devices are located when validating the active device list.
- (2) If a scanning tool is not available, use existing ICS documentation (inventory lists and schematics) to capture a list of assets deployed in the ICS.

b. Validate Active Hosts

- (1) Validate active hosts and locate inactive assets by walking through the ICS installation, documenting the assets located and how they are connected.

a. Create an ICS Topology Diagram, which includes the assets you located, the connections, IP addresses, and location of the asset using the tools made available by your command. Figure E-1 shows an example of an ICS Topology Diagram.

b. Store the ICS Topology Diagram in the binder entitled FMC Baseline Documents.

c. **NOTE:** For your site, ensure your diagram includes IP addresses, make and model of device, and operating system.

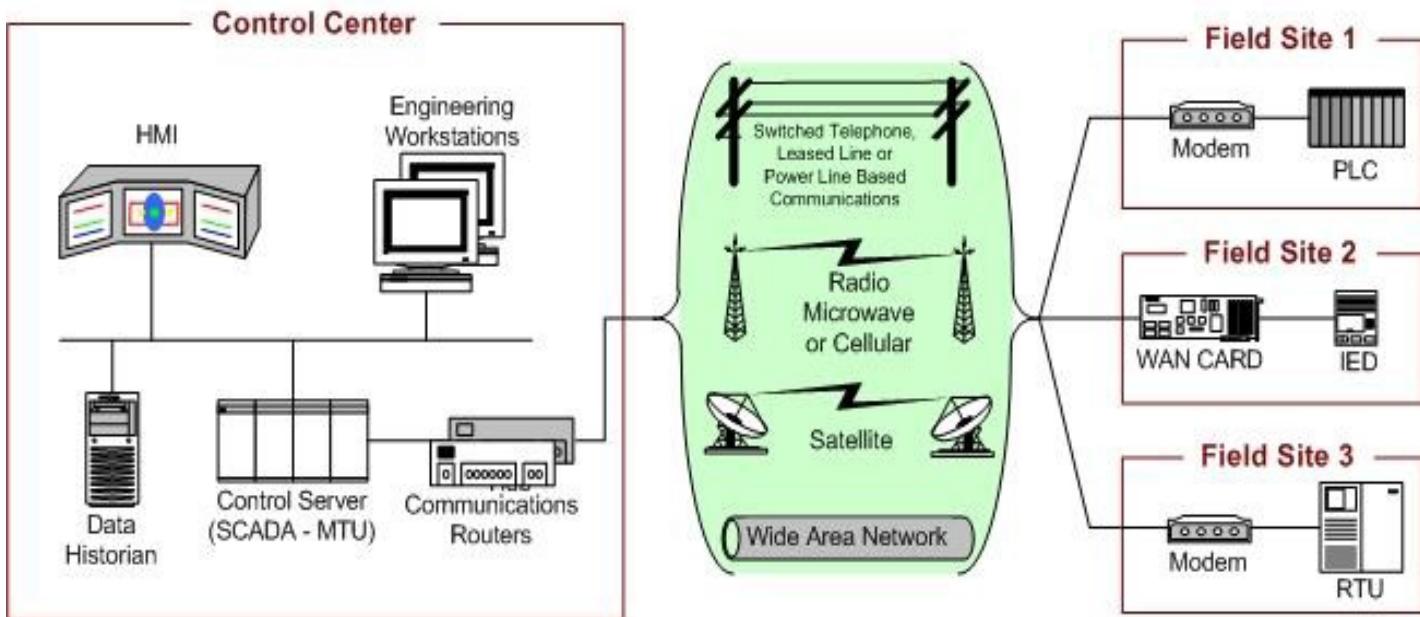


Figure E-1: SCADA system general layout from NIST SP 800-82.R2

E.5. FMC Baseline Creation: ICS Enclave Entry Points

What you will need:

1. ICS Topology.
2. **FMC Baseline Documents** binder
3. Vendor documentation or Help web pages for devices being listed in the table.

- a. From the next page, extract Table E-1: ICS Enclave Entry Points (make as many copies as needed). Insert this table (and copies) into FMC Baseline Documents binder.
- b. Use the ICS topology to identify all devices that provide entry to the ICS enclave from external networks. This can be a router or firewall connecting the command's enterprise, virtual private network (VPN) connections (possibly connecting to an engineering workstation), wireless connections, and any asset vendors use to connect from corporate locations to the ICS.
- c. Go to the identified devices, and extract the information required by the table using the instructions for that device.
- d. Enter the information into the table in the appropriate columns. See example table E-2 that follows table E-1.
- e. After completing the table, store it in the FMC Baseline Documents binder.

Command Name:**ICS Point of Contact:**

*Open Systems Interconnection (OSI)

Enclave Entry Point Baseline						
ICS Entry Point Device	IP and MAC Address	OSI* Layer	External Device	IP/MAC Address	OSI* Layer	Expected Ports, Protocols Used in This Connection
	IP: MAC:			IP: MAC:		In Out
	IP: MAC:			IP: MAC:		In Out
	IP: MAC:			IP: MAC:		In Out
	IP: MAC:			IP: MAC:		In Out
	IP: MAC:			IP: MAC:		In Out
	IP: MAC:			IP: MAC:		In Out
	IP: MAC:			IP: MAC:		In Out
	IP: MAC:			IP: MAC:		In Out
	IP: MAC:			IP: MAC:		In Out

Table E-1: ICS Enclave Entry Points

Enclave Entry Point Baseline						
ICS Entry Point Device	IP and MAC Address	OSI Layer	External Device	IP/MAC Address	OSI Layer	Expected Ports, Protocols Used in This Connection
Firewall	IP: 198.168.1.1	2	Command border router	IP: 192.168.1.1	3	Port: 179; protocol: BGP; Port: 22; protocol: SSH
	MAC: 00-13-84-EE-21-F4			MAC: 00-14-78-EE-19-F8		
Secondary Historian	IP: 192.168.1.150	3	Primary Historian	IP: 198.168.1.032	2	Port: 80; protocol HTTP Port: 118; protocol: SQL
	MAC: 00-32-20-EE-21-D4			MAC: 00-24-80-GG-C2		

Table E-2: Example ICS Enclave Entry Points

E.6. FMC Baseline Creation: Servers/Workstations

What you will need:

1. Formatted Write Once—Read Many media (either CD-r or DVD-r).
2. *Position Zero publication from the Information Assurance Directorate of the National Security Agency.*

- a. Create the FMC Baseline for servers and workstations (to include HMIs, Historians, OPCs, and Engineering Workstations) by performing the following tasks:
 - b. Procedures
 - (1) Preparation
 - (a) If you are not familiar with the Windows Command Prompt, review page 4-5 in NSA Publication, *Position Zero*, the Information Assurance Directorate of the National Security Agency/Central Security Services. See Appendix D: References.
 - (b) Use a formatted CD-r or DVD-r (hereafter referred to as “media”) to store the information you are collecting from servers and workstations. Label the media with the date the contents were collected, and provide a description of the contents on the label.
 - (c) If the asset you are inspecting does not have an abbreviated name, create one (e.g., HMI-Bld1) and use this to label electronic files that you will store on the media.
 - (d) Ensure you have administrator rights for the asset from which you are capturing data.
 - (e) **Important:** Enable Security Logging, specifically “user log-on” and “administrator log-on” for both the operating system and applications on the asset (procedures vary for differing systems, refer to vendor documentation).
 - (2) Data Capture
 - (a) Capture System Information:
 1. Insert media into the appropriate drive.
 2. Ensure the machine recognizes the drive by clicking on My Computer icon. Locate the media and note drive letter assigned to the drive (e.g., E:\)
 3. Open a command prompt.
 4. At the command prompt type: c:\> systeminfo > (media drive letter):\asset name-SysInfo.txt
Example: c:\>systeminfo >E:\HMI-Bld1-SysInfo.txt
 5. See *Position Zero*, from the Information Assurance Directorate of the National Security Agency/Central Security Services for more information about this command and output.
 - (b) Capture Task List
 1. Continue using the inserted media, and execute the following command to capture the machine’s Task List:
c:\> tasklist > (media drive letter):\asset name-Tasklist.txt

Example: c:\>tasklist > E:\HMI-BLD1-Tasklist.txt

2. See *Position Zero*, from the Information Assurance Directorate of the National Security Agency/Central Security Services for more information about this command and output.
- (c) Capture Processes and Dynamic Link Libraries (.dll)
 1. Continue using the inserted media, and execute the following command to capture the machine's processes and associated .dll:
c:\ tasklist /m /fo list >(media drive letter):\asset name-Proc-dll.txt
Example: c:\>tasklist /m /fo list > E:\HMI-BLD1-Proc-dll.txt
Alternately, run **listdlls** and save the output to a text file.
(see section EE.7 subsection D for details).
 2. See *Position Zero*, from the Information Assurance Directorate of the National Security Agency/Central Security Services for more information about this command and output.
- (d) Capture Services
 1. Continue using the inserted media, and execute the following command to capture the machine's running services:
c:\> tasklist /svc >(media drive letter):\asset name-Svc.txt
Example: c:\>tasklist /svc >E:\HMI-BLD1-Svc.txt
 2. Baseline full image paths for all services using reg query and output the results to a file (note: type following command on one line):
reg query HKLM\SYSTEM\CurrentControlSet\Services /s /t
REG_EXPAND_SZ >> service-image-paths.txt

e.g.

```
C:\>reg query HKLM\SYSTEM\CurrentControlSet\Services /s /t
REG_EXPAND_SZ

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\1394ohci
  ImagePath    REG_EXPAND_SZ
  \SystemRoot\system32\drivers\1394ohci.sys

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ACPI
  ImagePath    REG_EXPAND_SZ    system32\drivers\ACPI.sys

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AcpiPmi
  ImagePath    REG_EXPAND_SZ
  \SystemRoot\system32\drivers\acpipmi.sys
...[snip]...
```

(e) [Handle](#) (Microsoft SysInternals)

<https://docs.microsoft.com/en-us/sysinternals/downloads/handle>

This is a command line utility. Send the output to a text file. Document the results for potentially targeted ICS applications or services.

handle >> output.txt

Example:

```
C:\temp>handle
```

```
Nthandle v4.11 - Handle viewer
Copyright (C) 1997-2017 Mark Russinovich
Sysinternals - www.sysinternals.com

-----
System pid: 4 \<unable to open process>
  4C: File (R--)  C:\Program Files (x86)\Common
Files\Antivirus-Shared\EENGINE\EPERSIST.DAT
  58: File (R--)  C:\Windows\System32\config\TxR\{00000000-
0000-0000-0000-
000000000001}.TMContainer00000000000000000000000000000001.regtrans-ms
  60: File (R--)  C:\Windows\System32\config\TxR\{00000000-
0000-0000-0000-
000000000002}.TMContainer00000000000000000000000000000002.regtrans-ms
  80: File (RW-)  \clfs
  84: File (---)  C:\Windows\System32\config\RegBack\SYSTEM
  94: File (R--)  C:\System Volume Information\EfaData\
Antivirus.DB
  A4: File (RW-)  \clfs
  A8: File (RWD)  \clfs
  AC: File (RWD)  \clfs
  B0: File (RWD)  C:\$Extend\$RmMetadata\$Txf
  B4: File (R--)  \clfs
  B8: File (R--)  C:\$Extend\$RmMetadata\$TxfLog\$TxfLogContainer00000000000000000000
01
  BC: File (R--)  C:\$Extend\$RmMetadata\$TxfLog\$TxfLog.blf
  C0: File (RWD)  \clfs
  C4: File (RWD)  C:\Windows\System32\catroot\{00000000-0000-
0000-0000-000000000000}
```

[snip]

3. See *Position Zero*, from the Information Assurance Directorate of the National Security Agency/Central Security Services for more information about this command and output.
- (e) Capture Connecting Systems (Network Status)
1. Continue using the inserted media, and execute the following command to capture the machine's network status:
`c:\> netstat -ano >(media drive letter):\asset name-NetStat.txt`
Example: `c:\>netstat -ano > E:\HMI-BLD1-NetStat.txt`
 2. See *Position Zero*, from the Information Assurance Directorate of the National Security Agency/Central Security Services for more information about this command and output.

(f) Capture User Accounts

1. Continue using the inserted media, and execute the following command to capture the machine's network status:
c:\> net user >(media drive letter):\asset name-User.txt
Example: c:\>net user > E:\HMI-BLD1-User.txt

Alternately, use the WMIC useraccount command:

e.g.

```
C:\temp>wmic useraccount list full

AccountType=512
Description=Local Built-In Administrator Account
Disabled=TRUE
Domain=BLAH-PC
FullName=Administrator
InstallDate=
LocalAccount=TRUE
Lockout=FALSE
Name=Administrator
PasswordChangeable=TRUE
PasswordExpires=TRUE
PasswordRequired=TRUE
SID=S-1-5-21-00000000000-0000000000-00000000-1001
SIDType=1

...[snip]...
```

2. Review the file created in step 6.a. in Note Pad, and document users on the Authorized Users Table (table E-3). Duplicate table as needed.

(g) Local host file (DNS)

1. Calculate the hash value for the local Windows (or Linux/Unix) host file:
See Appendix E, section EE.2 for details.

(h) Mode command for serial ports.

1. Open the command prompt and run the mode command. Save the results.
e.g.

```
C:\temp>mode com1
```

Status for device COM1:

```
-----
Baud:      1200
Parity:    None
Data Bits: 7
Stop Bits: 1
Timeout:   OFF
XON/XOFF:  OFF
CTS handshaking: OFF
DSR handshaking: OFF
DSR sensitivity: OFF
DTR circuit: ON
RTS circuit: ON
```

This page intentionally left blank.

User Accounts for: _____ [asset name]				
Asset	User ID	User Name	Account Privileges	Normal log on times
			Guest User Admin	
			Guest User Admin	
			Guest User Admin	
			Guest User Admin	
			Guest User Admin	
			Guest User Admin	
			Guest User Admin	
			Guest User Admin	
			Guest User Admin	
			Guest User Admin	
			Guest User Admin	
			Guest User Admin	

Table E-3: Authorized Users Table

This page intentionally left blank.

E.7. FMC Baseline Creation: Network Traffic

- a. Capturing the normal data flow for the ICS provides a baseline view of the traffic that is “normal” for that ICS. The network traffic of an ICS should not be overly “busy” and should appear logical and reasonable to the operators (e.g., the OPC server and the field controllers should show communications between each other). Once the normal network traffic is captured and understood, identifying anomalous traffic is a straightforward event.
- b. Procedures
 - (1) If your ICS has Cisco devices, locate those devices and determine if those devices are NetFlow enabled (check Cisco web site).
 - (a) If the Cisco devices are NetFlow enabled, locate the device on the topology and determine what potential traffic can be viewed from that device (which device connections flow through the device).
 - (b) Using your Cisco documentation, determine how to capture network flows, and view these. To effectively baseline your network, allow NetFlow to capture 24 hours of ICS network traffic. Once the 24-hour network traffic has been captured, analyze the traffic and identify the individual IP addresses, the ports, protocols, services, and typical flows per day associated with these, and document them in table E-4: *ICS Data Flow*.
 - (2) If your ICS does not have Cisco devices, a variety of free tools can be used to capture data flows on the network. Work with your command's network administrator and the ISSM for assistance in installing these tools and capturing your ICS data flows.
 - (a) Select a method to capture network data, and capture the data for 24 hours. Analyze data, and populate table E-4 with IP addresses, ports, protocols, services, and typical flows per day identified during the capture.
 - (b) The following tools are free and can be used to capture network data flows: NetworkMiner, Microsoft Network Monitor, BandwidthD, PRTG Network Monitor Freeware, Splunk, ntopng, Wireshark.
 - (3) Extract table E-4 from this document and enter the IP addresses, ports, protocols , services, and typical flows per day, identified in the data flow capture.

This page intentionally left blank.

ICS Data Flows					
Originating IP	Destination IP	Port	Protocol	Service	Typical Flows/Day

Table E-4: ICS Data Flow

This page intentionally left blank.

ENCLOSURE F: JUMP-KIT

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

F.2. Jump-Kit Contents

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

Jump-Kit Contents: Documentation

- Incident Notifications List: document contact information for command's Information Assurance Manager
- Document stakeholders who could be affected by a Cyber attack on ICS
- Establish notification procedures with chain of command
- IT and ICS system schematics

Jump-Kit Contents: Tools

- Universal serial bus (USB) drives, USB optical (CD/DVD) drive, bootable USB (or LiveCD) with up-to-date anti-malware, and other software tools that can read and/or write to file system (Example: Bart's PE disk, or "Windows to Go" for Windows 10 environments)
- Laptop with anti-malware utilities and Internet access (for downloads)
- Computer and network tool kit to add/remove components, hard drives, connectors, wire cables, etc.
- Hard disk duplicators with write-block capabilities to capture hard drive images

Jump-Kit Contents: Configuration Files

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

F.3. Jump-Kit Maintenance

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.

F.4. Jump-Kit Rescue CD

The Rescue CD is a bootable CD with tools including: anti-malware/anti-virus utilities (with latest signatures), rootkit detection, master boot record check, and other capabilities.

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

- a. It is important to document environmental observations of what the device is doing, its symptoms and anomalies, and if the device is currently running or shut down. It is also important to note who has had access to the device and what the person did—if any actions were taken. Also, include documents for each step that is taken while acquiring data for forensics. This includes the following:
 - (1) Information on the specific device (i.e., make, model, identification number, location, etc.)
 - (2) The tools or utilities used to capture the data
 - (3) The commands or steps that were taken
 - (4) The device used to store the data
 - (5) If the data was collected remotely or locally
 - (6) The person that gathered the data
 - (7) Date and time in which the data was collected

G.3. Data Collection Tools

- a. Mandiant Redline
- b. Mandiant Memorize

- c. Microsoft SysInternals
- d. Microsoft Windows system utilities
- e. Linux system utilities

G.4. Capturing Memory Data

- a. Volatile Memory. Volatile memory is computer memory that requires power to maintain the stored information; it retains its contents while powered on, but when the power is interrupted the stored data is immediately lost.
- b. Non-Volatile Memory. Non-volatile computer memory is stored data that can be retrieved even after having the power cycled. Examples of non-volatile memory include read-only memory, flash memory, most types of magnetic computer storage devices and hard disks, floppy disks, magnetic tape, and optical discs.

G.5. Windows Registry Data

- a. The registry on a Microsoft Windows operating system is a database of configuration data used by the operating system and applications.
- b. The Registry Consists of Five Root Hives
 - 1. HKEY_CLASSES_ROOT
 - 2. HKEY_CURRENT_USER
 - 3. HKEY_LOCAL_MACHINE
 - 4. HKEY_USERS
 - 5. HKEY_CURRENT_CONFIG
- c. Cells of the Registry
 - 1. Key Cell
 - 2. Value Cell
 - 3. Subkey List Cell
 - 4. Value List Cell
 - 5. Security Descriptor Cell
- d. Windows Registry Tools
 - 1. [RegRipper](https://regripper.wordpress.com/): <https://regripper.wordpress.com/>
 - 2. RegEdit: Windows Utility
 - 3. Reg: Windows Utility
 - 4. [NirSoft Utilities](http://www.nirsoft.net/utils/regscanner.html): <http://www.nirsoft.net/utils/regscanner.html>
 - 5. [OSForensics](http://www.osforensics.com/download.html): <http://www.osforensics.com/download.html>
 - 6. [AutoRuns](https://docs.microsoft.com/en-us/sysinternals/) SysInternals: <https://docs.microsoft.com/en-us/sysinternals/>

ENCLOSURE H: MITIGATION ISOLATION AND PROTECTION

H.1. Isolation and Protection Introduction

- a. Description. Isolation and protection are two approaches to segmenting an ICS environment. Isolation contains an infected or compromised device, network segment, or other grouping of ICS assets. Protection ensures that critical ICS assets are protected from other compromised parts of the ICS system.
- b. Key Components
 - (1) Mitigation strategy
 - (2) Network diagrams
 - (3) Process dependencies
- c. Prerequisites
 - (1) Knowledge of networks
 - (2) Knowledge of processes

H.2. Isolation and Protection Overview

- a. The Mitigation Phase is meant to assist in protecting ICS during or after a cyber attack. There are two aspects to Mitigation: (1) containment and segmentation, and (2) establishing control to ensure end-state processes continue to operate. Containment and segmentation are the procedures for separating one asset, or group of assets, from other assets or networks.
 - (1) Isolation segments the affected assets to prevent it from affecting other assets. For example, if an HMI workstation were compromised, the workstation would be disconnected from the network. This would contain or limit the malware or malicious activity to that one workstation.
 - (2) Protection is the process of segmenting the ICS systems from other systems to prevent compromise to the ICS system, prevent exfiltration of data, and to sever command and control by outside actors. For example, if the SCADA network were compromised, the ICS network and the removal of a network cable connecting the two networks at a firewall, switch, or router could segment the SCADA network. This would protect the ICS network.
- b. In many cases you will want to perform both segmentation and containment, isolating the infected assets and protecting the ICS process and end devices.
- c. All Mitigation steps should be performed with an understanding of the impact the segmentation will have on operational systems and processes.

H.3. Creating a Segmentation Strategy

- a. The segmentation strategy is a documented process for understanding how your ICS assets could be separated during and after a cyber attack. Each ICS environment is unique, based on protocols, network architecture, physical locations, equipment, software, and mission priorities.
- b. The first step is to identify the commander's mission priorities. These are the most critical processes that must remain operational.
- c. The second step is to identify critical processes and dependencies. This includes identifying all of the assets that are required to keep the mission priorities operational.
- d. The third step is to review the network architecture to identify logical points where segmentation could occur to contain infected assets or protect the ICS processes.
- e. This document should be maintained with the continuity of operations and baseline documentation.

H.4. Suggested Segmentation Areas

- a. Enclave Segmentation. Enclave segmentation is the separation of accreditation boundaries. The enclave is a collection of information systems connected by one or more internal networks under the control of a single authority and a security policy. The systems may be structured by physical proximity or by function. (CNSSA-4009)
- b. Network Segmentation. Information technology segmentation (network segmentation) is the division of a large network into smaller networks or network segments.
- c. Zone and Conduit Segmentation. Industrial Control Systems may be separated based on zones and conduits. Zone segmentation is the division of industrial systems into grouped sub-systems for the primary purpose of reducing the attack surface and minimizing attack vectors. It limits the flow of data between zones. (Knapp, 2015)
 - (1) Physical zones are defined based on the grouping of assets based on physical location.
 - (2) Logical zones are grouped based on a particular functionality or characteristic.
- d. ICS Process Segmentation. The ICS process segmentation is designed around an ICS process like power, water, HVAC, etc. The ICS process segmentation separates one process from another process.
- e. Device Mitigation. The device segmentation is meant to assist operators in isolating an affected or targeted device that is stand alone, or out-of-band, which does not communicate with other devices. This is the least intrusive Mitigation action to an ICS system. This procedure should be used when evidence of an adversarial presence is identified and limited to a single device.
- f. Network Virtual LAN (VLAN). VLANs are created to subdivide a network into virtual network segments. This architecture provides additional security. When VLANs are implemented, they provide an additional location for segmentation.
- g. Sub-system. The sub-system segmentation is meant to assist operators in isolating a targeted or affected sub-system or function. The three main segments of an ICS are field devices, field controllers, and HMIs. These work together for a specific process or

function. For example, one sub-system may be used for power, another for water treatment. The purpose of sub-system Mitigation is to isolate and maintain local control of a particular function without affecting the remainder of the system.

- h. Layer. The ICS layer segmentation is meant to assist operators in isolating a targeted or affected ICS network within an information system. These Mitigation actions are the most intrusive and should be undertaken when the incident is rapidly propagating and is potentially targeting lower layers, or when the ISSM and the operators believe that the ICS devices and processes at the lower levels are being directly threatened.

This page intentionally left blank.

ENCLOSURE I: CYBER SEVERITY LEVELS

I.1. Cyber Severity Levels Introduction

- a. **Description.** Cyber Severity Levels are a designation of the extent to which cyber activity may impact the operational mission or supporting operational requirements.
- b. **Key Components**
 - (1) CJCSM 6510.01B, *Cyber Incident Handling Program*, December 2014 (appendix A, section AA.15)
 - (2) Severity Levels
 - (3) Malicious Actions

I.2. Cyber Severity Levels Overview

While ICS/SCADA can be attacked in a variety of ways, there are a number of steps that are common, or at least present in most attacks. Each of these steps could yield some behavioral change in the system that could be detected by an operator. However, not all Detections require a Mitigation action. Mitigation is a disruptive process, which could degrade the operational capabilities. Given those circumstances, a more graduated approach to Detection/Mitigation allows IT and ICS managers to take steps to assess the cyber event to determine what level of response is required and react proportionately. Table I-1 provides the incident level severity rating approach used in the ACI TTP.

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

I.4. Precedence and Category Levels

CJCSM 6510.01B provides guidance to DoD components on routine cyber events. Further, the manual states in section 1.a.(3) that in the event of emergencies and active hostilities, USCYBERCOM will provide additional guidance. The ACI TTP provides that additional guidance to ICS operators for the handling of cyber events during active hostilities or emergencies.

However, to ensure consistent reporting and integration with the cyber incident/event chain of command, the ACI TTP will characterize cyber incidences/events using the CJCSM 6510.01B Precedence and Category Levels Table (table I-2). This table represents the precedence and category levels located throughout the ACI TTP. The table is provided for informational purposes, as the ACI TTP characterizes cyber incidents and events within the reporting schemas.

Precedence	Category	Description
0	0	Training and Exercises
1	1	Root-Level Intrusions (Incident)
2	2	User-Level Intrusion (Incident)
3	4	Denial of Service (Incident)
4	7	Malicious Logic (Incident)
5	3	Unsuccessful Activity Attempt (Event)
6	5	Non-compliance Activity (Event)
7	6	Reconnaissance (Event)
8	8	Investigating (Event)
9	9	Explained Anomaly (Event)

Table I-2: Precedence and Category Levels Table (CJCSM 6510.01B)

I.5. Malicious Actions Table

The Malicious Actions Table (table I-3) provides actions and the resulting Severity Level.

Action	Description	Category	Severity Level
Malicious Reconnaissance	Anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability	6	2
Phishing Attack	A method of causing a user with legitimate access to an information system, or information that is stored on, processed by, or transiting an information system, to unwittingly enable the defeat of a security control or exploitation of a security vulnerability	7	3

Action	Description	Category	Severity Level
Malicious Command and Control	Method for unauthorized remote identification of, access to, or use of, an information system or information that is stored on, processed by, or transiting an information system	7	3
Exfiltration	Information is leaked and used by an attacker	7	3
Defeating a Security Control	Compromising a physical or logical system security control	7	3
Exploitation of a Vulnerability	Something that takes advantage of a bug or vulnerability in order to cause unintended or unanticipated behavior	7	3
Unsuccessful Activity Attempt	Unsuccessful logon attempts	3	2
Degradation	Performance impact; means that performance can be measured before or after event	7	3
Denial of Service (DOS)	Asset, system, or process unavailable for a period of time. A DOS within an ICS network is more serious than an external DOS attack	4	Internal-3 External-2
Modification	Data, file system, software, and/or packets were altered; set points either at rest or in transit	2	3
Injection	Introduce suspect or malicious information into a system	1	3
Unauthorized Use	Resources used for attackers own purposes; also, resources inappropriately used by a person in a position of trust	2	3

Table I-3: Malicious Actions Table

This page intentionally left blank.

APPENDIX A: SUPPORTING MATERIALS

AA.1 System Characterization Guidelines

The baselining guidelines located in enclosure E were designed to assist information technology (IT) and industrial control system (ICS) managers in characterizing the ICS (also known as developing a baseline). This baseline should be used as a reference during the execution of the Detection phase of the tactics, techniques, and procedures (TTP).

While executing the Detection phase of the Advanced Cyber Industrial Control System Tactics, Techniques, and Procedures (ACI TTP) during a cyber event, IT and ICS operators can compare a system's state to its baseline, and determine whether:

- a. A system is connected to the correct assets
- b. A system is executing the correct processes
- c. A system is allowing the correct users access at the correct permission level during normal working hours
- d. The network traffic is normal
- e. The security settings or configuration files have been altered on the system
- f. The firmware properties have been altered

These guidelines consist of tables that can be populated as well as instructions for tools that commonly exist on most systems located in the ICS. Tools are used to generate text files that contain information about the ICS baseline. These files can either be printed and stored as hard copies or stored on magnetic media. In either case, the idea is to maintain this information in a safe and readily available manner.

AA.2 Characterizing ICS (Establishing the Baseline)

Effective Detection of an adversary's actions requires an understanding of what a system's normal operations are. Characterizing the ICS, also known as establishing the baseline, allows IT and ICS managers to document normal conditions for the ICS, and store these for reference during the execution of the Detection portion of the TTP. Without such information, Detecting the activity of an advanced cyber adversary would prove very difficult.

The following artifacts should be included in the ICS baseline:

- a. Network architecture diagram
- b. Data flows
- c. Authorized list of software and hardware
- d. Configuration files
- e. Firmware values
- f. Authorized ports, protocols, and services
- g. User accounts with authorized privileges

Guidelines and templates required to characterize the ICS are located in this appendix.

AA.3 Collaborating with Network Managers and Establishing Restoration Point

The enterprise (or network) perimeter devices, such as firewalls, perimeter routers, demilitarized zones (DMZ), et cetera, which form (in most cases) the corporate enterprise facing layer of the ICS, is managed by the command's information technology (IT) organization.

These devices may or may not be configured to Detect attack signatures that could affect the ICS (such as inbound/outbound ICS-specific protocols). Therefore, the ICS organization should engage the command's IT organization and develop a concept of operations relative to the network perimeter, and the ICS' cyber security needs.

In addition to coordinating with the command's IT organization, the ICS organization should coordinate with the ISSM, and obtain the command's notification procedures for cyber events.

If the ICS has undergone any type of Certification and Accreditation (C&A), whether platform IT (PIT) or a full C&A package, a variety of documents should be available establishing the fully mission-capable (FMC) baseline.

AA.4 Routers and Switches

While routers are not often located within an ICS network, they are commonly located within corporate networks, specifically connecting two wide area networks (WANs) or connecting a WAN to the Internet. However, wireless routers do commonly connect ICS to remote devices or vendors.

Routers and switches can be configured in a variety of ways. It is important to establish the FMC baseline of ICS routers and switches. The hash for the router and switches Internetwork Operating System (IOS) should be captured and stored with the Recovery Jump-Kit. In addition, the firmware hash, as well as the router and switch configuration file, should be captured and stored. The IOS should be available on vendor-provided media. If not, the IOS and firmware should be downloaded from the vendor's web site, stored onto magnetic media, and write-protected. The date and time, as well as the versions of the IOS and firmware, should be logged.

AA.5 Servers and Workstations

There are several servers and workstations commonly located within an ICS. These include data historians, human-machine interfaces (HMIs), application servers, data base servers, and engineering workstations. Each of these machines provides a variety of opportunities for exploitation. It is important to create an International Organization for Standardization (ISO) image of each machine to be stored in the Recovery Jump-Kit. An ISO image is an archive file composed of the data contents from every written sector of a device. In addition, the basic input and output system (BIOS) hash should be captured and stored with the Recovery Jump-Kit.

AA.6 Network Architecture

The Recovery Jump-Kit should always include the network architecture diagram. This architecture documents which devices are connected, what external connections exist, and how these devices are connected. The network architecture should include:

- a. Internet Protocol (IP) addresses for each device
- b. MAC addresses for each device
- c. Connection means (e.g., Ethernet, serial connection, etc.)
- d. Device names and location

Ideally, the network architecture would be created using a network scanning tool. However, if such a tool is not available, the network should be mapped by using command line interface commands and physically “walking the wires,” which refers to a manual process of tracing connections manually and documenting their location, ports, and connectivity.

AA.7 Data Flow Diagrams

Understanding what information should be flowing through the ICS is a key data point when attempting to identify malicious actors hiding within the network traffic. A data flow diagram should be included in the Jump-Kit in order to provide operators with a baseline understanding of their normal flow of network traffic. While data flows can change with new software releases and updates, overall, ICS data flows should remain fairly constant and predictable. Data flow diagrams include: where data is flowing from and where data is flowing to, and documentation of the ports, protocols, and services.

AA.8 Authorized User List

As with the network architecture and the data flow diagrams, understanding who should be on the ICS and what they should be permitted to access also provides a baseline picture of how the ICS should be operating.

If an operator discovers a new account on an ICS asset, and that account is not linked to an authorized user, or if an authorized user is using his/her account in an abnormal manner, these may be signs of a malicious actor spoofing a user account. Having a list of authorized users and what they are permitted to access provides operators with a known, good baseline of authorized users, and it enables operators to recognize malicious actors who are spoofing accounts.

AA.9 Notifications

Keeping command stakeholders advised of a cyber incident allows all parties to remain vigilant relative to their own systems. Cyber attacks, particularly those coming from well-funded and motivated actors, have specific objectives in mind, and are trying to degrade a command’s capability in order to achieve a larger objective. Providing relevant information about a cyber

attack up and down the chain of command ensures every potentially affected entity within the chain of command is informed and ready to defend the network in their area of cognizance.

While the Department of Defense (DoD) maintains overarching notification requirements for cyber incidences, each service and subordinate command may have unique notification requirements. ICS operators should become familiar with these requirements and integrate these into their standard notification procedures.

At a minimum, ICS operators should identify those individuals and organizations that are responsible for networking infrastructure, cyber security, incident response plans, and notification requirements.

AA.10 Training Requirements and Recommendations

To enhance the effective use of the ACI TTP, it is recommended that the following training be completed by anyone who plans to use the ACI TTP:

ICS Training

ICS-CERT VLP: Virtual Learning Portal provides free online courses. The following courses are recommended:

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

A certification of completion is available after completing all modules. These courses are available for access at the following URL:

<https://ics-cert-training.inl.gov/Pages/Catalog/CourseCatalog.aspx>

In addition to the recommended free online courses, there are other courses and certifications that would be beneficial. However, some of these are not free and not available online.

- Global Industrial Cyber Security Professional (GICSP) Certification
- SANS ICS410: ICS/supervisory control and data acquisition systems (SCADA) Security Essentials Training
- GIAC Response and Industrial Defense (GRID) Certification
- SANS ICS515: ICS Active Defense and Incident Response Training
- ICS-CERT: Introduction to Control Systems Cybersecurity (101)
- ICS-CERT: Intermediate Cybersecurity for Industrial Control Systems (201)

- ICS-CERT: Intermediate Cybersecurity for Industrial Control Systems (202)
- ICS-CERT: ICS Cybersecurity (301)
- SCADAHacker: Understanding, Assessing and Securing Industrial Control Systems
- INFOSEC Institute: Certified SCADA Security Architect
- ISASecure: Embedded Device Security Assurance Certification
- ISASecure: System Security Assurance Certification
- ISASecure: Security Development Lifecycle Certification

Security Training

The National Defense University (NDU) is a national security institution focused on advanced joint education and leader development and scholarship. NDU supports the joint warfighter by providing rigorous Joint Professional Military Education to members of the U.S. Armed Forces and select others in order to develop leaders that have the ability to operate and creatively think in an unpredictable and complex world. Information can be found at <http://www.ndu.edu/>.

IT Training

DoDD 8140.01 (formerly DoD 8570.01-m) Cyber Workforce Management Program provides guidance for the identification and categorization of positions and certification of personnel conducting cyberspace work roles within the DoD workforce supporting the DoD Information Network (DODIN). The DoD cyberspace workforce includes, but is not limited to, all individuals performing any of the functions described in DoDD 8140.01.

Table AA-1 lists a number of IT courses/certifications that meet the DoD baseline certifications for the cyberspace Workforce.

Carnegie Mellon Software Engineering Institute CERT® *	Computer Security Incident Handler (CSIH)
Cisco	Cisco Certified Network Associate-Security (CCNA-Security)
Computing Technology Industry Association (CompTIA) *	A+ Continuing Education (CE)
CompTIA *	Security+ Continuing Education (CE)
CompTIA *	CompTIA Advanced Security Practitioner Continuing Education (CE)
CompTIA *	Network+ Continuing Education (CE)
EC-Council *	Certified Ethical Hacker (CEH)
International Information Systems Security Certifications Consortium (ISC)2 *	Certified Information Systems Security Professional (CISSP) (or Associate – this means the individual has qualified for the certification except for the number of years of experience)

(ISC)2 *	Certified Secure Software Lifecycle Professional
(ISC)2 *	Certification Authorization Professional (CAP)
(ISC)2 *	Information Systems Security Architecture Professional (ISSAP)
(ISC)2 *	Information Systems Security Engineering Professional (ISSEP)
(ISC)2 *	Information Systems Security Management Professional (ISSMP)
(ISC)2 *	System Security Certified Practitioner (SSCP)
Information Systems Audit and Control Association (ISACA) *	Certified Information Security Manager (CISM)
ISACA *	Certified Information Systems Auditor (CISA)
Global Information Assurance Certification (GIAC) *	GIAC Certified Intrusion Analyst (GCIA)
GIAC *	GIAC Certified Enterprise Defender (GCED)
GIAC *	GIAC Certified Forensic Analyst (GCFA)
GIAC *	GIAC Certified Incident Handler (GCIH)
GIAC *	GIAC Security Essentials Certification (GSEC)
GIAC *	GIAC Security Leadership Certificate (GSLC)
GIAC *	GIAC Systems and Network Auditor (GSNA)
GIAC *	GIAC Global Industrial Cyber Security Professional (GICSP)

Table AA-1: Certifications / Courses**AA.11 ICS Position Responsibilities**

The intent of this section is to provide suggested responsibilities of individuals normally associated with the operation of ICS. These positions may exist under different names; however, their roles should be applicable to roles within the ACI TTP. Given that a cyber incident involving ICS systems will affect the critical operational capabilities of a command, establishing clear lines of communication with command stakeholders is key to the successful management of a cyber incident.

- a. Chief of Operations:
 - (1) Serve as the senior member of the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), as well as the interface with senior management.
 - (2) Assume operational control of all members of the ICS-CERT during an event.
 - (3) Provide final decision-making capability on operational matters in the event of an ICS cyber incident.
 - (4) Institute the ICS incident response plan (IRP), and supervise throughout the process.

- (5) Assign the duty of incident response team lead.
 - (6) Provide subject matter expertise in the area of Operations to IT personnel.
 - (7) Serve as the interface between the organization and outside response entities/government agencies.
- b. Chief Information Officer (CIO):
- (1) Serve as the senior member of the IT personnel on the ICS team, and provide the chief of operations with guidance in mitigating cyber incidents from an IT standpoint.
 - (2) Provide the chief of operations with information pertaining to the cyber incident attack vector, how it was Detected, and what actions should be conducted to Mitigate its affects.
 - (3) Provide IT personnel with guidance, and supervise their actions during an ICS cyber incident.
 - (4) Oversee the IT portion of the IRP, and ensure IT personnel are adhering to its procedures.
 - (5) Ensure IT personnel are interfacing with ICS personnel, and provide updates to the chief of operations as appropriate.
 - (6) Supervise the ICS-CERT risk management process, and serve as its designated official.
- c. Security Manager:
- (1) Provide the Chief of Operations with subject matter expertise in the area of physical security and security policy during a cyber incident.
 - (2) Ensure enhanced force protection conditions (FPCONs) are instituted and enforced during an event.
 - (3) Determine if any assets were physically compromised during or preceding the incident as well as level of criticality, and communicate this to the chief of operations.
 - (4) Supervise and task security personnel operating in the field, and provide them with managerial-level expertise in the conduct of their duties.
 - (5) Work in conjunction with the ICS, IT, and information assurance managers to coordinate efforts and provide a full-spectrum response to an incident.
 - (6) Supervise the ICS-CERT risk management process.
- d. Information Systems Security Manager (ISSM):
- (1) Continually communicate the information assurance (IA) common operating picture (COP) to the CIO.
 - (2) Provide the CIO with subject matter expertise in the area of IA during a cyber incident.
 - (3) Ensure enhanced information operations conditions (INFOCONs) are instituted and enforced during a cyber incident.
 - (4) Determine what the information impacts of the event are, and report them to the CIO.
 - (5) Supervise and task IA technicians operating in the field, and provide them with managerial-level expertise in the conduct of their duties.

- (6) Work in conjunction with the ICS, IT, and security managers to coordinate efforts and provide a full-spectrum response to an incident.
 - (7) Coordinate the ICS-CERT Risk Management process.
- e. IT Manager:
- (1) Continually communicate the IT COP to the CIO.
 - (2) Provide the CIO with subject matter expertise in the area of IT during a cyber incident.
 - (3) Determine the IT assets compromised by the incident as well as level of criticality, and communicate this to the CIO.
 - (4) Make recommendations to the CIO on the IT actions necessary to Mitigate a cyber incident.
 - (5) Supervise and task IT technicians operating in the field and provide them with managerial-level expertise in the conduct of their duties.
 - (6) Ensure technicians are following the IRP as indicated and completing necessary tracking paperwork as appropriate.
 - (7) Work in conjunction with the ICS, IA, and security manager to coordinate efforts and provide a full-spectrum response to an incident.
 - (8) Prior to an event during the ICS-CERT risk management process, inventory and define information technology assets to assist in determining criticality, vulnerabilities, threats, and overall risk. Develop an information systems and network map.
 - (9) Assist ICS personnel in determining interdependencies and additional vulnerabilities posed by IT/ICS systems.
- f. ICS/Plant Manager:
- (1) Continually communicate the ICS COP to the chief of operations.
 - (2) Provide the chief of operations with subject matter expertise in the area of Information Assurance during a cyber incident.
 - (3) Determine the ICS assets and processes affected by the incident as well as their level of criticality and communicate this to the chief of operations.
 - (4) Determine the Recoverability Level of the process/machine and communicate this to the chief of operations.
 - (5) Make recommendations to the chief of operations on the ICS actions necessary to Mitigate a cyber incident.
 - (6) Supervise and task ICS engineers and operators in the field and provide them with managerial-level expertise in the conduct of their duties.
 - (7) Ensure engineers and operators are following the IRP per the ACI TTP as indicated, and complete necessary tracking paperwork as appropriate.
 - (8) Work in conjunction with the IT, IA, and security manager to coordinate efforts and provide a full-spectrum response to an incident.
 - (9) Prior to an event during the ICS-CERT risk management process, inventory and define ICS assets to assist in determining criticality, vulnerabilities, threats, and overall risk. Develop an ICS system map and, if feasible, an ICS process diagram.

(10) Assist IT personnel in determining interdependencies and additional vulnerabilities posed by IT/ICS systems.

g. Controls Engineer:

- (1) Continually communicate any changes to ICS machines and processes to the ICS manager.
- (2) Provide the ICS/plant manager with tactical-level expertise of the tactical procedures necessary to Mitigate negative effects to ICS machines and processes.
- (3) Determine the functional impacts of the cyber incident and communicate this to the ICS/plant managers.
- (4) Oversee and conduct the tactical-level implementation of the ACI TTP necessary to Mitigate the incident.
- (5) Supervise and lead the actions of ICS operators, and provide them with tactical-level expertise in the ACI TTP, necessary to Mitigate the event.
- (6) Supervise the actions of any ICS vendors responding to the incident.
- (7) It is recommended that the Controls Engineer successfully complete the following ICS-CERT virtual learning portal courses:

- 100W - OPSEC for Control Systems
- 210W - Cybersecurity for Industrial Control Systems

See Appendix A: Supporting Material, AA.10, Training Requirements and Recommendations, for additional information.

- (8) Follow the IRP per the ACI TTP, and complete necessary tracking paperwork as appropriate.

h. IT Technician:

- (1) Continually communicate any changes to IT assets to the ICS manager.
- (2) Provide the IT manager with tactical-level expertise of the procedures necessary to Mitigate negative effects to IT assets.
- (3) Determine the functional impacts of the cyber incident to IT assets, and communicate this to the IT manager.
- (4) Determine the Recoverability Level of the IT Assets and communicate this to the IT manager.
- (5) Conduct the tactical-level implementation of the ACI TTP necessary to Mitigate the incident.
- (6) Supervise the actions of any IT vendors responding to the incident.
- (7) It is recommended that the IT Technician comply with DoDD 8140.01 (formerly 8570.01) at an IAT Level 1 or higher.

See Appendix A: Supporting Materials, AA.10. Training Requirements and Recommendations, for additional information.

- (8) Follow the IRP per the ACI TTP and complete necessary tracking paperwork as appropriate.

- i. ICS Operator:
 - (1) Continually communicate any changes to ICS assets to the controls engineer.
 - (2) Provide the control engineer with field-level expertise of the procedures necessary to Mitigate negative effects to ICS assets.
 - (3) Conduct the ACI TTP necessary to Mitigate the effects of a cyber incident.
 - (4) It is recommended that the ICS operator successfully complete the following ICS-CERT virtual learning portal courses:
 - 100W - OPSEC for Control Systems
 - 210W - Cybersecurity for Industrial Control SystemsSee Appendix A: Supporting Materials, AA.10, Training Requirements and Recommendations, for additional information.
 - (5) Follow the IRP per the ACI TTP and complete the necessary tracking paperwork as appropriate.
- j. Vendor/Service Representatives:
 - (1) Provide equipment-specific subject matter expertise to ICS-CERT personnel.
 - (2) Assist in the Mitigation of cyber incidents if necessary.
 - (3) Provide the ICS-CERT team with the equipment-specific tools, hardware, software, and firmware necessary to Mitigate an event.

AA.12 Cyber Incident Analysis Tools

One source of tool information is the Defense Cyber Crime Center (DC3) on-line site located at www.dc3.mil/technical-solutions/tools. DC3 Tools are for U.S. DoD and Federal law enforcement and counterintelligence (LE/CI) official use only. To access these tools, authorized personnel may submit a request to DCCI@dc3.mil.

AA.13 Cyber Incident Documentation

Once a potential attack has been Detected and verified, all steps should be documented in the Security Log as a continuation of the event that was started in the Detection phase to identify any actions taken, observations made, symptoms identified, and/or individuals who may have had contact with the system.

AA.14 Cyber Incident Reporting

Incident reporting is a framework for the timely notification of any reportable cyber event or incident. Reporting provides indicators of adversary reconnaissance, probing, intrusions, network exploitations, and attacks. It is important to relay all pertinent incident information to the ISSM for appropriate reporting. The cyber incident reporting process is documented in CJCSM 6510.01B (section AA.15).

AA.15 Integration with CJCSM 6510.01B Requirements

- a. Mitigation consists of short-term tactical actions to stop an intruder's access to a compromised information system, limit the extent of an intrusion, prevent an intruder from causing further damage, and allow the system to remain in some state of operation.
 - (1) The primary objectives for the Mitigation procedures are:
 - (a) Regain control of the information systems involved in order to further analyze the cyber incident, allow for continued operations, and eventually return the IT to normal operation.
 - (b) Deny an intruder access to prevent him or her from continuing the malicious activity and from affecting other information systems and data.
 - (2) While an intruder has access to an information system, the information system cannot be properly analyzed or restored. Performing Mitigation:
 - (a) Prevents an intruder from accessing or exfiltrating DoD data or other information.
 - (b) Prevents an intruder from destroying valuable evidence and tampering with information systems while they are being analyzed.
 - (c) Prevents an intruder from using DoD information systems to attack other information systems.
 - (d) Allows an organization to continue operations in some manner.
 - (3) Mitigation provides a reasonable security solution until sufficient information is collected to address the vulnerabilities exploited and the damage sustained.
 - (a) It should be noted that some Mitigation actions could be taken during the preliminary response phase of the incident-handling life cycle.
 - (b) More Mitigation steps may be warranted following in-depth analysis, which may identify more affected information systems or malicious activities. Mitigation steps can be executed iteratively with the steps in the Detection and analysis phases.
 - (4) Mitigation strategies are executed by the organization responsible for the maintenance and operation of the affected DoD information networks or information systems. In this organization it could be a local system administrator or could be the component's CNDSP. Who executes the strategies will depend on the incident type and affected component and local policy and procedures.
- b. Appendix E of CJCSM 6510.01B (section AA.15 of this TTP) states that one of the strategies for effectively addressing a cyber incident is that of "Mitigation."

This page intentionally left blank.

APPENDIX B: ACRONYMS AND ABBREVIATIONS

Acronym or Abbreviation	Definition
ACI TTP	Advanced Cyber Industrial Control System Tactics, Techniques, and Procedures
ACL	access control list
ASA	adaptive security appliance
BIOS	basic input and output system
C&A	certification and accreditation
CCNA	Cisco Certified Network Associate
CD	compact disk
CE	continuing education
CEH	Certified Ethical Hacker
CIA	confidentiality, integrity, and availability
CIO	Chief Information Officer
CISSP	Certified Information Systems Security Professional
CJCSM	Chairman of Joint Chiefs of Staff Manual
CNDSP	computer network defense service provider
COA	course of action
COP	common operating picture
CPT	cyber protection team
CPU	central processing unit
CSIH	Computer Security Incident Handler
DC3	Defense Cyber Crime Center
DCS	distributed control system
DLL	dynamic link library
DMZ	demilitarized zone
DNP3	distributed network protocol
DoD	Department of Defense
DoDI	Department of Defense Instruction
DODIN	Department of Defense Information Network
DOS	denial of service
DVD	digital versatile disc
FMC	Fully Mission-Capable
FPCON	force protection condition
FTP	file transfer protocol
GICSP	Global Industrial Cyber Security Professional
HMI	human-machine interface
HTTP	hypertext transfer protocol
HTTPS	secure hypertext transfer protocol
HVAC	heating, ventilation, and air conditioning
IA	information assurance
ICS	industrial control systems
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
IDS	intrusion detection system
IED	Intelligent electronic device
INFOCON	information operations condition

Acronym or Abbreviation	Definition
IOS	Internetwork Operating System
IP	Internet Protocol
IRP	Incident Response Plan
ISO	International Organization for Standardization
ISSM	Information Systems Security Manager
IT	information technology
J-BASICS	Joint Base Architectures for Secure Industrial Control Systems
JT	Joint Test
LAN	local area network
MAC	media access control
MTU	master terminal unit
NDU	National Defense University
NMap	Network Mapper
NSA	National Security Agency
NIPRNet	Non-secure Internet Protocol Router Network
NIST	National Institute of Standards and Technology
OLE	object linking and embedding
OPC	object linking and embedding (OLE) for process control
OPSEC	operational security
OSI	Open Systems Interconnection
PIT	platform information technology
PLC	programmable logic controller
RMF	risk management framework
RTU	remote terminal unit
SIEM	security information and event management
SCADA	supervisory control and data acquisition systems
SMTP	simple mail transfer protocol
SP	special publication
TFTP	trivial file transfer protocol
TTP	tactics, techniques, and procedures
URL	uniform resource locator
USB	universal serial bus
USCYBERCOM	United States Cyber Command
VLAN	virtual local area network
VLP	Virtual Learning Portal
VPN	virtual private network
WAN	wide area network
WARNORD	Warning Order

APPENDIX C: DEFINITIONS

Access Control List — A mechanism that implements access control for a system resource by enumerating the identities of the system entities that are permitted to access the resources. (OMB Circular A-130, 1996)

Application — A computer program with an interface enabling people to use the computer as a tool to accomplish a specific task.

Baseline — A minimum starting point used for comparisons.

Baseline Topology — A diagram of the network and network devices as it should be. This is compared to the as-is state of the network to identify any changes that have been made.

Breach — A security breach is any incident that results in unauthorized access of data, applications, services, networks, and/or devices by bypassing their underlying security mechanisms.

Cybersecurity — Prevention of damage to, protection of, and restoration of, computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

Cyber Attack — Actions taken through the use of a computer to target information systems or computer networks to disrupt, deny, manipulate, or destroy information.

Field Controllers — Field Controllers collect and process input and output (I/O) data. They also send the process data to the HMI. The field controller is one of the three main segments of an ICS.

Field Devices — Equipment that is connected to the field side on an ICS. Examples of field devices include RTUs, PLCs, actuators, sensors, and HMIs. A field device is one of the three main segments of an ICS.

Human-Machine Interface (HMI) — An HMI is the user interface in a process control system. It provides a graphics-based visualization of an industrial control and monitoring system. The HMI is one of the three main segments of an ICS.

ICS Manager — An individual who typically oversees industrial operations, focusing on product quality, environmental protection, and industrial safety. Creates and maintains automated building control systems that regulate temperature, lighting, humidity, water, and electricity as well as automated industrial control systems. Calibrates machines, troubleshoots equipment, and repairs or replaces instruments.

Intelligent Electronic Device (IED) — Any device incorporating one or more processors with the capability to receive or send data/control from or to an external source (e.g., electronic multifunction meters, digital relays, controllers).

IT Manager — The individual responsible for the information system infrastructure related to the ICS. This includes enclave perimeter devices, network backbone, servers, and workstations.

Local Control — The ability to maintain overall functionality of the endpoint devices with the controller segregated from the wider network.

Malicious Actor — A threat that poses a possible danger that might exploit a vulnerability to breach security and damage systems.

Malicious Command and Control — A method for unauthorized remote identification of, access to, or use of, an information system or information that is stored on, processed by, or transiting an information system.

Malicious Reconnaissance — A method for actively probing or passively monitoring an information system for the purpose of discerning security vulnerabilities of the information system, if such method is associated with a known or suspected cybersecurity threat. (S. 754)

Malware — Software that was designed and produced to damage or disable computers and computer systems.

Network Scanner — A program that attempts to find security vulnerabilities in one or more systems connected to a network.

Operators — An individual who operates either SCADA or ICS equipment.

Programmable Logic Controller (PLC) — A solid-state control system that has a user-programmable memory for storing instructions for the purpose of implementing specific functions such as I/O control, logic, timing, counting, three mode (PID) control, communication, arithmetic, and data and file processing. (RFC 4949, 2007)

Reintegration — The careful, methodical reconnection of devices on a segregated network to fully functioning operation.

Remote Terminal — A computer with radio interfacing used in remote situations where communications via wire is unavailable. Usually used to communicate with remote field equipment. (NIST Special Publication 800-39)

Rootkit — A rootkit is a collection of files that is installed on a system to alter the standard functionality of the system in a malicious and stealthy way. The rootkit may hide evidence of its existence and the changes made to the system. Rootkits are often used to install other types of malware. (NIST Special Publication 800-83)

Security Control — The management, operational, and technical controls used to protect against an unauthorized effort to adversely affect the confidentiality, integrity, and availability of an information system or its information. (S. 754)

Supervisory Control and Data Acquisition (SCADA) — A generic name for a computerized system that is capable of gathering and processing data and applying operational controls over long distances. Typical uses include power transmission and distribution and pipeline systems. SCADA was designed for the unique communication challenges (e.g., delays, data integrity) posed by the various media that must be used, such as phone lines, microwave, and satellite. Usually shared rather than dedicated. (RFC 4949, 2007)

Threat — An action, not protected by the First Amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system. (S. 754)

WARNORD — Warning Order issued by the United States Cyber Command in response to a suspected cyber attack.

This page intentionally left blank.

APPENDIX D: REFERENCES

- Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6211.02. (current edition). *Defense Information System Network (DISN) Responsibilities*.
- CJCSM 6510.01B. (December 18, 2014). *Cyber Incident Handling Program*.
- Committee on National Security Systems Policy 22. (January 2012). *Policy on Information Assurance Risk Management for National Security Systems*.
- Department of Defense Directive (DoDD) 3020.40. (January 14, 2010). *DoD Policy and Responsibilities for Critical Infrastructure*.
- Department of Defense Instruction (DoDI) 5200.44. (November 5, 2012). *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)*.
- DoDD 8530.1. (January 8, 2001). *Computer Network Defense (CND)*.
- DoDI 5205.13. (January 29, 2010). *Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA) Activities*.
- DoDI 8500.01. (March 14, 2014). *Cybersecurity*.
- DoDI 8510.01. (March 12, 2014). *Risk Management Framework (RMF) for DoD Information Technology (IT)*.
- DoDI 8551.1. (August 13, 2004). *Ports, Protocols, and Services Management (PPSM)*.
- Independent Safeguarding Authority. (October 16, 2002). *Automation, Systems, and Instrumentation Dictionary*. 4th Edition. <https://www.isa.org>.
- Knapp, Eric. (2011). *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*. Waltham, MS. Syngress.
- Ligh, Michael. (2014). *The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory*.
- National Institute of Standards & Technology (NIST). Special Publication 800-39. (current edition). *Managing Information Security Risk: Organization, Mission, and Information System View*.
- NIST. Special Publication 800-82 Rev. 2 (May 2015). *Guide to Industrial Control Systems (ICS) Security*. <https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final>.
- NIST. Special Publication 800-147. (current edition). *Basic Input/Output System (BIOS) Protection Guidelines*.
- NSA, Information Assurance Directorate. (2015). *Position Zero: Integrity Checking Windows-Based ICS/SCADA Systems*.

Office of Management and Budget. Circular A-130. (February 8, 1996). *Managing Federal Information as a Strategic Resource*.
<https://www.federalregister.gov/documents/2016/07/28/2016-17872/revision-of-omb-circular-no-a-130-managing-information-as-a-strategic-resource>.

Shirey, R. Request for Comments: 4949. (August 2007). *Internet Security Glossary, Version 2*.
<https://tools.ietf.org/html/rfc4949>.

U.S. Senate. S. 754. (current version). *Cybersecurity Information Sharing Act of 2015*.
<https://www.congress.gov/bill/114th-congress/senate-bill/754>.

White House. (January 8, 2008). *National Security Presidential Directive-54/Homeland Security Presidential Directive-23, Cybersecurity Policy*. <http://fas.org/irp/offdocs/nspd/nspd-54.pdf>.

APPENDIX E: Technical Supplement

Command Line Instructions

Introduction

Many of the instructions in this section require the use of the Windows Command Prompt interface. To open the Windows Command Prompt, from the Windows menu select: Start, Run, type cmd, and press enter.

Please note that there is a predominance of Microsoft Windows focused recommendations in this guide. Although specific ICS hardware may or may not operate on Windows or Embedded Windows, the software that is used to administer this hardware is most likely running on Windows. As more ICS systems begin to use other operating systems this guide will be updated. Some of the included guidance is not OS specific but is more procedure oriented. In many cases, the Windows focused guidance and concepts discussed will often apply to other operating systems as well (with minor adjustments to command line syntax and/or file names/locations).

In some cases, multiple methods are given to detect the same type of malicious activity. Some of these methods require software not included by default in a Windows installation (e.g. Microsoft SysInternals Utilities). If the environment does not allow for these utilities, use one of the default Windows utilities options instead.

EE.0 Microsoft's SysInternals utilities

Some of these instructions require the use of Microsoft's SysInternals utilities. These diagnostic and troubleshooting utilities for the Microsoft Windows platform are not installed by default.

More information and access to the utilities can be found at the following links:

SysInternals website:

<https://docs.microsoft.com/en-us/sysinternals/>

Download for entire suite:

<https://docs.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite>

Download for individual utilities:

<https://docs.microsoft.com/en-us/sysinternals/downloads/>

Online version of the tools:

<https://live.sysinternals.com/>

Depending on your organization's environment, you may need to download the SysInternals utilities to a CD/DVD or network share, or in some case run them "live" from the online webpage.

EE.1 Check Windows Registry “Run” Keys

Description:

The Windows “Run” Registry keys are used by Windows to automatically start programs at login (either at every login or just one time). Malicious software (malware) can take advantage of these keys to initiate certain actions or enable persistence on a system. The “reg query” command can be used to display the content of these keys.

Command:

At the command prompt, enter the following four commands (separately).

```
reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Run  
reg query HKCU\Software\Microsoft\Windows\CurrentVersion\Run  
reg query HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce  
reg query HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce
```

Example:

```
C:\>reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Run
```

Results:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run  
    SAVUpdate      REG_SZ      %comspec% /c  
    "C:\Radiatmp\AdminScripts\ADGroupToLocalGroup.exe"  
        picon      REG_SZ      "C:\Program Files (x86)\Common  
Files\Intel\Privacy Icon\PIconStartup.exe" -startup  
        ac.activclient.gui.scagent.exe    REG_SZ      "C:\Program  
Files\ActivIdentity\ActivClient\ac.activclient.gui.  
scagent.exe"  
        test-bad1    REG_SZ      C:\temp\bad1.exe
```

Review the results that are displayed. Note the unexpected “bad” key and “bad” value shown in red font in the example results. It is recommended to have a baseline of values to compare against in order to determine if results match expected values.

EE.2 Check Integrity of Local DNS Host File

Description:

The Domain Name System (DNS) service is used to provide a mapping of computer host names to IP addresses (similar to a phone book). Normally, DNS services are provided by a DNS server over the network. However, Windows also has a local Domain Name System (DNS) host file that can be used to provide similar functionality. Entries in this local DNS file will take priority over the network DNS service. Malware will sometimes modify this local DNS file in order to provide false mappings between host names and IP addresses. There are number of reasons that this may be done; one goal can be to redirect a user's network traffic to a malicious server. It is unusual in an enterprise environment for this local host file to change or be modified from the default/baseline configuration.

One method that can be used to check the integrity of a file is to run an algorithmic hash (e.g. MD5, SHA) on the file and then compare the hash value against the hash of a baseline/known good file.

The default location of the Windows host file is: %systemroot%\System32\drivers\etc\hosts

Windows contains a default utility (CertUtil) that can be used to perform the hashing.

Command:

```
CertUtil -hashfile \directory\path\to\filename HashAlgorithm
```

Note: in the command above, replace “\directory\path\to\” with the directory path to the file and replace “filename” with the file’s name. Also specify the hash algorithm of MD5 (or whichever hash format is specified in the baseline to which you will be comparing the file against).

Example:

```
C:\>CertUtil -hashfile %systemroot%\System32\drivers\etc\hosts MD5
```

Results:

```
MD5 hash of file C:\Windows\System32\drivers\etc\hosts:
```

```
36 88 37 43 25 b9 92 de f1 27 93 50 03 07 56 6d
```

```
CertUtil: -hashfile command completed successfully.
```

Compare the hash of this file to the hash of a known good host file (from the same OS/version/patch level or “baseline”) to see if they match.

If the hashes do not match, review the contents of the host file for any unauthorized entries.

Note that hash values may be displayed in segments as shown above or may appear as one long string of characters (e.g. [3688374325b992def12793500307566d](#)) . The format of these values should be treated as equivalent.

EE.3 Check Local DNS Host file registry path

Description:

Another method by which malware can manipulate DNS is to alter the path to the local DNS host file in the Windows Registry. If this registry value were altered to a non-standard location, then a second malicious host file could be created at that location and this “impostor” host file would then be used by Windows rather than the authentic host file. The imposter host file could contain malicious host entries and, due to the path change, any checks performed against the original host file would not detect the imposter host file or its entries. The “reg query” command can be used to display the content of the relevant key that would display this change.

Command/Example:

```
C:\>reg query HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
```

Result:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
  ICSDomain      REG_SZ      mshome.net
  SyncDomainWithMembership   REG_DWORD     0x1
  NV Hostname      REG_SZ      w7core-xd033
  DataBasePath    REG_EXPAND_SZ    %SystemRoot%\System32\drivers\etc
  NameServer      REG_SZ
  ForwardBroadcasts  REG_DWORD     0x0
  IPEnableRouter   REG_DWORD     0x0
  Domain          REG_SZ      MITRE.ORG
  Hostname        REG_SZ      w7core-xd033
  SearchList       REG_SZ      MITRE.ORG
  UseDomainNameDevolution REG_DWORD     0x1
  EnableICMPRedirect REG_DWORD     0x1
  DeadGWDetectDefault REG_DWORD     0x1
  DontAddDefaultGatewayDefault REG_DWORD     0x0
  EnableWsd        REG_DWORD     0x1
  QualifyingDestinationThreshold REG_DWORD     0x3
```

Review the value of "DataBasePath" to see if it matches: %SystemRoot%\System32\drivers\etc

EE.4 Hidden Alternate Data Stream (ADS) files

Description:

Alternate Data Stream (ADS) files are a special type of file in Windows that does not display in standard views or with default commands. These hidden files are in a sense “embedded” as a part of another file. Even an algorithmic hash of an original file may not detect the presence of an embedded ADS file. These hidden characteristics makes this type of file format very attractive for malware.

There is a Microsoft SysInternals utility called [Streams](#) (not installed by default) which can display and/or remove this type of file. There is also a switch option for the standard Dir command which can display these files.

Note: There are legitimate uses for the ADS file format and presence of an ADS file is not necessarily an indicator of malware. Be sure to review the contents of the actual ADS file to determine validity.

Command (using SysInternals [Streams](#)):

```
streams.exe -s C:\test-subdir
```

The optional -s switch enables a recursive search (i.e. search subdirectories).

Example:

```
C:\test-subdir>streams.exe -s C:\test-subdir
```

Results:

```
Streams v1.56 - Enumerate alternate NTFS data streams
Copyright (C) 1999-2007 Mark Russinovich
Sysinternals - www.sysinternals.com
```

```
C:\test-subdir\target.txt:
:hide.txt:$DATA 11
```

Hidden ADS file is detected (see red font).

If it is not permissible to install the [Streams](#) utility, the native Windows “dir” command can also be used.

Command:

```
dir /R /s
```

The /R switch enables the ADS detection; the optional /s switch enables a recursive search (i.e. search subdirectories). Note: When searching large directories, it is recommended to redirect the output to a file (e.g. dir /R /s >>output.txt). This will allow for easier searching on the following string: :\$DATA

Example:

```
C:\test-subdir>dir /R
```

Results:

```
Volume in drive C has no label.  
Volume Serial Number is 1A20-98E7
```

```
Directory of C:\test-subdir
```

```
09/02/2016  11:16 AM    <DIR>          .  
09/02/2016  11:16 AM    <DIR>          ..  
09/02/2016  11:17 AM    <DIR>        originals  
09/02/2016  11:38 AM            47 target.txt  
                                11 target.txt:hide.txt:$DATA  
                                47 bytes  
1 File(s)                 47 bytes  
3 Dir(s)   884,519,604,224 bytes free
```

The hidden ADS file is detected (see red font).

EE.5 "Health" Checks for Antivirus, Host Based/EndPoint Protection Software

Description:

Among the first targets for malware to attack on a host are the following: Antivirus, Host Intrusion Prevention/EndPoint Protection software.

It is recommended that the “health” of this software be monitored routinely through automated reporting or (if need be) through manual processes as shown below. Also verify that the services associated with the software are running and that the software’s “signatures” are current.

Commands:

Use the “sc query” command to get a list of the relevant software services.

(Note that the spaces after the “=” signs are required)

```
C:\>sc query type= service state= all | find /i "[product name]"
```

Examples:

For Symantec:

```
C:\>sc query type= service state= all | find /i "symantec"
```

For McAfee:

```
C:\>sc query type= service state= all | find /i "mcafee"
```

Results:

```
DISPLAY_NAME: Symantec Endpoint Protection
DISPLAY_NAME: Symantec Network Access Control
```

Note that "long/display names" for these services are returned.

Next, use the “sc GetKeyName” commands to get the "short names" (used by the registry) for these services.

Example:

```
C:\>sc GetKeyName "Symantec Endpoint Protection"
```

Results

```
[SC] GetServiceKeyName SUCCESS
Name = SepMasterService
```

```
C:\>sc GetKeyName "Symantec Network Access Control"
[SC] GetServiceKeyName SUCCESS
Name = SNAC
```

Next use the "sc query" command (in conjunction with the results of the "short names" from the previous step) to get the status of the services.

Example:

```
C:\>sc query SepMasterService
```

Results:

```
SERVICE_NAME: SepMasterService
    TYPE          : 10  WIN32_OWN_PROCESS
    STATE         : 4   RUNNING
                  (NOT_STOPPABLE, NOT_PAUSABLE,
ACCEPTS_SHUTDOWN)
    WIN32_EXIT_CODE : 0  (0x0)
    SERVICE_EXIT_CODE : 0  (0x0)
    CHECKPOINT      : 0x0
    WAIT_HINT       : 0x0
```

Example:

```
C:\>sc query SNAC
```

Results:

```
SERVICE_NAME: SNAC
    TYPE          : 10  WIN32_OWN_PROCESS
    STATE         : 1   STOPPED
    WIN32_EXIT_CODE : 1077  (0x435)
    SERVICE_EXIT_CODE : 0  (0x0)
    CHECKPOINT      : 0x0
    WAIT_HINT       : 0x0
```

Command above shows detection of the "STOPPED"; determine if this is the intended state.

For McAfee/HBSS, the queries to run are as follows:

```
sc query McShield
sc query McTaskManager
sc query McAfeeFramework
sc query mfevtp
sc query McAfeeAuditManager
sc query mfefire
sc query enterceptAgent
```

Description:

Antivirus definitions date check.

If automated reporting (of the currently installed) antivirus DAT/definition dates is not available, obtain the currently version via a command line registry query.

Command/Example:**For Symantec:**

```
C:\>reg query "HKLM\Software\Symantec\Symantec Endpoint Protection\CurrentVersion\public-opstate"
(Type all one line and use quotes on this query due to the spaces in the path.)
```

Results:

```
HKEY_LOCAL_MACHINE\Software\Symantec\Symantec Endpoint Protection\CurrentVersion\public-opstate
ContentDownloadHealth      REG_DWORD      0x1
LatestVirusDefsDate       REG_SZ        2016-09-30
LatestVirusDefsRevision    REG_DWORD      0x2
AVRunningStatus           REG_DWORD      0x1
ASRunningStatus           REG_DWORD      0x1
p2p_enabled               REG_DWORD      0x0
snac_enabled               REG_DWORD      0x0
FWRunningStatus           REG_DWORD      0x1
.
.
.
```

Note the date shown in red font above.

Alternate Command/Example:

```
C:\>reg query "HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\CurrentVersion\SharedDefs"
(Use quotes on this query due to the spaces in the path.)
```

Results:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\CurrentVersion\SharedDefs
NAVCORP_70      REG_SZ      C:\ProgramData\Symantec\Symantec Endpoint Protection\12.1.7004.6500.105\Data\Definitions\VirusDefs\20160930.002
DEFWATCH_10     REG_SZ      C:\ProgramData\Symantec\Symantec Endpoint Protection\12.1.7004.6500.105\Data\Definitions\VirusDefs\20160930.002
SRTSP          REG_SZ      C:\ProgramData\Symantec\Symantec Endpoint Protection\12.1.7004.6500.105\Data\Definitions\VirusDefs\20160930.002
```

Alternate Command/Examples:

For McAfee, use one or more of the following: (depending on the installed version):

```
reg query "HKLM\Software\Wow6432Node\McAfee\SystemCore\VScore\On  
Access Scanner\McShield"
```

(Use quotes on this query due to the spaces in the path.)

```
reg query HKLM\Software\Wow6432Node\McAfee\AVEngine
```

```
reg query HKLM\Software\McAfee\DesktopProtection
```

```
reg query HKLM\Software\Wow6432Node\McAfee\DesktopProtection
```

EE.6 Adjust Windows Policy to log use of command shell

Malware may attempt to manipulate a system by executing commands from an operating system's "shell" or command line. By default, opening of a Microsoft Windows command shell does not generate an event log entry; this makes monitoring for the activity difficult. It is possible to adjust Windows policy (in Windows 7 and later) to log this information to the Windows event log as security event ID 4688.

To enable the Audit Process Creation policy, edit the following group policy:

Policy location: Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Configuration > Detailed Tracking +

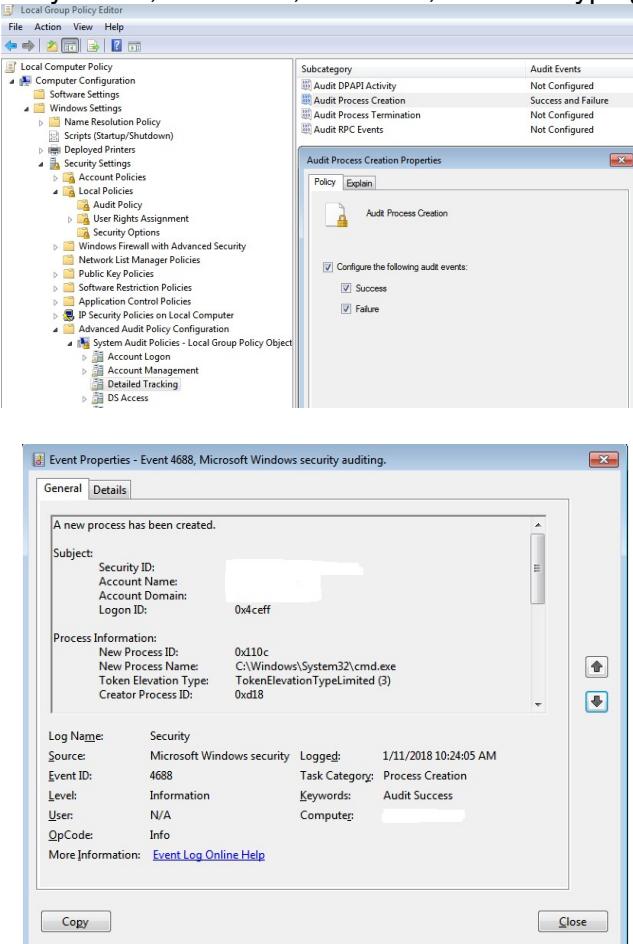
Policy Name: Audit Process Creation

[Path: Administrative Templates\System\Audit Process Creation

Setting: Include command line in process creation events]

Note: These last two lines may not be needed in Windows7

To open the Local Group Policy Editor, click Start, click Run, and then type gpedit.msc.



For additional details see:

<https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing>

Note: For a related item (PowerShell), see section EE.17

EE.7 Detect unknown processes, DLLs, EXEs, or threads

Malware may attempt to execute malicious processes on a targeted system. It is important to detect the appearance of these processes. Review currently running processes against baseline processes. Use one or more of the methods below.

If available, make use of Application Whitelisting capabilities, e.g. Windows AppLocker, Windows Defender Exploit Guard, Windows Defender Application Control, or 3rd party Whitelisting software. See following link for additional information on Application Whitelisting: <https://www.iad.gov/iad/library/ia-guidance/security-configuration/industrial-control-systems/guidelines-for-application-whitelisting-industrial-control-systems.cfm>

A. Compare services in the Registry to Baseline.

Review Registry Services keys:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services

Compare these Registry entries to the Baseline (see Enclosure E FMC Baseline, step E.6, section b.2.d)

Evaluate any differences that are discovered.

B. Microsoft “sc” utility

sc query type= service

Note: Consider piping this command to a file (due to large output)
(note “=” has to be directly adjacent to “type”...no space)

e.g.

sc query type= service

```

SERVICE_NAME: Appinfo
DISPLAY_NAME: Application Information
    TYPE          : 20  WIN32_SHARE_PROCESS
    STATE         : 4   RUNNING
                  (STOPPABLE, NOT_PAUSABLE,
IGNORES_SHUTDOWN)
    WIN32_EXIT_CODE  : 0  (0x0)
    SERVICE_EXIT_CODE : 0  (0x0)
    CHECKPOINT      : 0x0
    WAIT_HINT       : 0x0

SERVICE_NAME: AppMgmt
DISPLAY_NAME: Application Management
    TYPE          : 20  WIN32_SHARE_PROCESS
    STATE         : 4   RUNNING
                  (STOPPABLE, NOT_PAUSABLE,
IGNORES_SHUTDOWN)
    WIN32_EXIT_CODE  : 0  (0x0)
    SERVICE_EXIT_CODE : 0  (0x0)
    CHECKPOINT      : 0x0
    WAIT_HINT       : 0x0

SERVICE_NAME: AudioEndpointBuilder
DISPLAY_NAME: Windows Audio Endpoint Builder
    TYPE          : 20  WIN32_SHARE_PROCESS
    STATE         : 4   RUNNING

```

```

(STOPPABLE, NOT_PAUSABLE,
IGNORES_SHUTDOWN)
    WIN32_EXIT_CODE      : 0  (0x0)
    SERVICE_EXIT_CODE   : 0  (0x0)
    CHECKPOINT          : 0x0
    WAIT_HINT           : 0x0

SERVICE_NAME: AudioSrv
DISPLAY_NAME: Windows Audio
    TYPE              : 20  WIN32_SHARE_PROCESS
    STATE             : 4   RUNNING
                           (STOPPABLE, NOT_PAUSABLE,

```

[snip]

C. PsList

<https://docs.microsoft.com/en-us/sysinternals/downloads/pslist>
Compare output to baseline

e.g.

```
C:\temp>pslist
PsList v1.4 - Process information lister
Copyright (C) 2000-2016 Mark Russinovich
Sysinternals - www.sysinternals.com
```

Process information for MM198644-PC:

Name	Pid	Pri	Thd	Hnd	Priv	CPU Time	Elapsed Time
Idle	0	0	8	0	0	358:00:41.589	0:00:00.000
System	4	8	122	664	124	0:01:55.877	44:47:17.887
smss	284	11	3	36	812	0:00:00.078	44:47:17.887
csrss	412	13	9	777	3644	0:00:01.154	44:47:16.702
wininit	452	13	3	86	2504	0:00:00.062	44:47:16.468
csrss	468	13	10	593	3840	0:00:29.905	44:47:16.452
services	508	9	6	258	8368	0:00:02.574	44:47:16.343
winlogon	540	13	3	124	4712	0:00:00.156	44:47:16.249
lsass	552	9	7	784	10968	0:00:13.587	44:47:16.234
lsm	560	8	10	232	4748	0:00:00.218	44:47:16.234
svchost	680	8	9	400	6792	0:00:11.076	44:47:15.859
svchost	760	8	8	356	7128	0:00:02.012	44:47:15.750
svchost	860	8	19	861	41668	0:00:09.063	44:47:15.719
svchost	900	8	26	632	19276	0:00:00.655	44:47:15.688
svchost	948	8	17	382	17840	0:00:00.592	44:47:15.672
svchost	972	8	41	1319	31304	0:00:08.096	44:47:15.656
svchost	340	8	6	222	5460	0:00:00.483	44:47:15.563

[snip]

D. ListDLLs

<https://docs.microsoft.com/en-us/sysinternals/downloads/listdlls>
Run and compare output to baseline.

e.g.

```
C:\temp>listdlls
```

```
Listdlls v3.2 - Listdlls
Copyright (C) 1997-2016 Mark Russinovich
```

Sysinternals

```
Error opening System(4):
Access is denied.
```

```
-----
smss.exe pid: 284
Command line: \SystemRoot\System32\smss.exe
```

Base	Size	Path
0x0000000000000000	0x20000	C:\Windows\System32\smss.exe
0x0000000000000000	0x1aa000	C:\Windows\SYSTEM32\ntdll.dll

```
-----
csrss.exe pid: 412
Command line: %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows
SharedSection=1024
11=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3
ServerDll=winsrv:ConServerDll
Off MaxRequestThreads=16
```

Base	Size	Path
0x0000000000000000	0x6000	C:\Windows\system32\csrss.exe
0x0000000000000000	0x1aa000	C:\Windows\SYSTEM32\ntdll.dll
0x0000000000000000	0x13000	C:\Windows\system32\CSRSRV.dll
0x0000000000000000	0x11000	C:\Windows\system32\basesrv.DLL
0x0000000000000000	0x38000	C:\Windows\system32\winsrv.DLL
0x0000000000000000	0xfa000	C:\Windows\system32\USER32.dll
0x0000000000000000	0x67000	C:\Windows\system32\GDI32.dll

[snip]

E. PsService

<https://docs.microsoft.com/en-us/sysinternals/downloads/psservice>
(queries service status; can show service dependencies)

e.g.

```
C:\temp>psservice
PsService v2.25 - Service information and configuration utility
Copyright (C) 2001-2010 Mark Russinovich
Sysinternals - www.sysinternals.com

SERVICE_NAME: AdobeFlashPlayerUpdateSvc
DISPLAY_NAME: Adobe Flash Player Update Service
This service keeps your Adobe Flash Player installation up to date with the
latest enhancements and security fixes.
    TYPE          : 10 WIN32_OWN_PROCESS
    STATE         : 1 STOPPED
                  (NOT_STOPPABLE,NOT_PAUSABLE,IGNORES_SHUTDOWN)
    WIN32_EXIT_CODE : 1077 (0x435)
    SERVICE_EXIT_CODE : 0 (0x0)
    CHECKPOINT    : 0x0
    WAIT_HINT     : 0 ms

SERVICE_NAME: AeLookupSvc
DISPLAY_NAME: Application Experience
Processes application compatibility cache requests for applications as they are
launched
    TYPE          : 20 WIN32_SHARE_PROCESS
    STATE         : 4 RUNNING
                  (STOPPABLE,NOT_PAUSABLE,IGNORES_SHUTDOWN)
    WIN32_EXIT_CODE : 0 (0x0)
    SERVICE_EXIT_CODE : 0 (0x0)
```

```

CHECKPOINT      : 0x0
WAIT_HINT       : 0 ms

SERVICE_NAME: ALG
DISPLAY_NAME: Application Layer Gateway Service
Provides support for 3rd party protocol plug-ins for Internet Connection
Sharing
    TYPE          : 10 WIN32_OWN_PROCESS
    STATE         : 1 STOPPED
                  (NOT_STOPPABLE,NOT_PAUSABLE,IGNORES_SHUTDOWN)
    WIN32_EXIT_CODE : 1077 (0x435)
    SERVICE_EXIT_CODE : 0 (0x0)
    CHECKPOINT    : 0x0
    WAIT_HINT     : 0 ms
[snip]

```

F. Sigcheck

<https://docs.microsoft.com/en-us/sysinternals/downloads/sigcheck>

Sigcheck can help to provide insight into the validity of a file/process.

It can even work with VirusTotal.

It can scan all executable files (of any type) "sigcheck -e"

It can show certificates

e.g.

```
C:\Program Files (x86)\Adobe\Reader XX.0\Reader>c:\temp\sigcheck -e
```

```
Sigcheck v2.60 - File version and signature viewer
Copyright (C) 2004-2017 Mark Russinovich
Sysinternals - www.sysinternals.com
```

```
C:\Program Files (x86)\Adobe\Reader XX.0\Reader\A3DUtils.dll:
  Verified:      Signed
  Signing date: 8:16 AM 5/8/2014
  Publisher:    Adobe Systems, Incorporated
  Company:      Adobe Systems Incorporated
  Description:  3D Utilities Library 11.0
  Product:      3D Utilities Library
  Prod version: 11.0.07.79
  File version: 11.0.07.79
  MachineType: 32-bit

C:\Program Files (x86)\Adobe\Reader XX.0\Reader\ACE.dll:
  Verified:      Signed
  Signing date: 10:26 PM 9/23/2012
  Publisher:    Adobe Systems, Incorporated
  Company:      Adobe Systems Incorporated
  Description:  Adobe Color Engine
  Product:      ACE 2012/09/07-19:07:31
  Prod version: 78.517761
  File version: 2.20.02.1
  MachineType: 32-bit
```

G. Tasklist: (Also see section D.5, Steps 11-14, Routine Monitoring: Computer Assets)

- tasklist /svc shows services associated with each Windows process

e.g.

```
C:\>tasklist /svc
```

Image Name	PID	Services
System Idle Process	0	N/A
System	4	N/A
smss.exe	284	N/A
csrss.exe	412	N/A
wininit.exe	452	N/A
csrss.exe	468	N/A
services.exe	508	N/A
winlogon.exe	540	N/A
lsass.exe	552	KeyIso, ProtectedStorage, SamSs
lsm.exe	560	N/A
svchost.exe	680	DcomLaunch, PlugPlay, Power
svchost.exe	760	RpcEptMapper, RpcSs
svchost.exe	860	AudioSrv, Dhcp, eventlog, lmhosts, wscsvc
svchost.exe	900	AudioEndpointBuilder, CscService, dot3svc, hidserv, Netman, PcaSvc, TrkWks, UmRdpService, UxSms, wudfsvc
svchost.exe	948	EventSystem, FontCache, netprof, nsi, sppuinotify, WdiServiceHost

[snip]

tasklist /M [dll or exe name] shows all processes using a specified DLL or exe

e.g.

```
C:\>tasklist /m kernel32.dll
```

Image Name	PID	Modules
taskhost.exe	2928	kernel32.dll
dwm.exe	3328	kernel32.dll
explorer.exe	3352	kernel32.dll
RtDCp164.exe	3460	kernel32.dll
EMET_Agent.exe	3616	KERNEL32.dll
mspaint.exe	3544	kernel32.dll
cmd.exe	5892	kernel32.dll
conhost.exe	3876	kernel32.dll
tasklist.exe	6116	kernel32.dll

tasklist /m /fi "imagename eq [executable]" show dlls associated with a process:

e.g.

```
C:\>tasklist /m /fi "imagename eq cmd.exe"
```

Image Name	PID	Modules
cmd.exe	5892	ntdll.dll, kernel32.dll, KERNELBASE.dll, SYSFER.DLL, msrvct.dll, WINBRAND.dll, USER32.dll, GDI32.dll, LPK.dll, USP10.dll, IMM32.DLL, MSCTF.dll, apphelp.dll

H. WMIC:

Dump list of currently running processes to an html table for review (and comparison to baseline):

```
wmic /output:c:\[output directory]\[output file.html] process list /format:htable
```

e.g.

```
C:\>wmic /output:c:\temp\processList.html process list /format:htable
```

				1700.	88	156001				Microsoft Windows 7 E	C:\Windows\Device		
				1736.	118	156001				Microsoft Windows 7 E	C:\Windows\Device		
				1760.	1736	744748774				Microsoft Windows 7 E	C:\Windows\Device		
				1796.	739	24492157				Microsoft Windows 7 E	C:\Windows\Device		
				WmiPrvSE.exe.	2164.	230	145236931			WmiPrvSE.exe.	Microsoft Windows 7 E	C:\Windows\Device	
				svchost.exe.	2316.	113	312002			svchost.exe.	Microsoft Windows 7 E	C:\Windows\Device	
				unsecapp.exe.	2752.	72	0			unsecapp.exe.	Microsoft Windows 7 E	C:\Windows\Device	
				taskhost.exe.	C:\Windows\system32\taskhost.exe.	2928.	154	1404009	1380	taskhost.exe.	Microsoft Windows 7 E	C:\Windows\Device	
					C:\Program Files (x86)\	2472.	343	1092007	3072	1024		Microsoft Windows 7 E	C:\Windows\Device
				pppsvc.exe.	2988.	172	41652267			pppsvc.exe.	Microsoft Windows 7 E	C:\Windows\Device	
				dwm.exe.	C:\Windows\system32\dwm.exe.	3328.	82	156001	1380	200	dwm.exe.	Microsoft Windows 7 E	C:\Windows\Device
				explorer.exe.	C:\Windows\Explorer.EXE	3352.	1063	175345124	1380	200	explorer.exe.	Microsoft Windows 7 E	C:\Windows\Device
				RtDCp64.exe.	C:\Program Files\Realtek\Audio\HDA\RtDCp64.exe.	3460.	226	0	1380	200	RtDCp64.exe.	Microsoft Windows 7 E	C:\Windows\Device
				EMET_Agent.exe.	C:\Program Files (x86)\EMET 4.1\EMET_Agent.exe.	3616.	267	1716011	1380	200	EMET_Agent.exe.	Microsoft Windows 7 E	C:\Windows\Device

EE.8 Detect malware manipulation of legitimate processes

Malware may stop or kill, and then start legitimate processes in order to manipulate a system. Since “ungraceful” process stops/kills are not usually logged, it may be easier to use one or more of the following methods to detect subsequent/recent process starts/restarts. Recent process starts (outside of normal maintenance windows) for long running systems may indicate that malicious manipulation has occurred and this could warrant further review.

Also see Enclosure A, section A.2.5.

A. Powershell Get-Process cmdlet (requires admin):

<https://blogs.technet.microsoft.com/heyscriptingguy/2012/11/18/powertip-use-powershell-to-easily-see-process-start-time/>

example:

```
Get-Process | Select-Object id, name, starttime | Sort starttime
```

B. Powershell Get-Eventlog cmdlet

<https://www.coretechnologies.com/blog/windows-services/service-start-time/>

example for print spooler (use service's display name):

```
Get-EventLog -LogName "System" -Source "Service Control Manager" -EntryType "Information" -Message "*Print Spooler service*running*" -Newest 1
```

C. SC queryex command

1. First run: sc queryex [service/process name], and retrieve the PID

example (for windows firewall):

```
sc queryex MpsSvc
```

2. then run the following powershell query on the PID shown in the result from step 1

```
Get-Process | select name, id, starttime | select-string [PID from above]
```

D. WMIC (WMI command line tool)

```
WMIC PROCESS GET NAME, CREATIONDATE
```

E. PowerShell New-TimeSpan cmdlet

<https://blogs.technet.microsoft.com/heyscriptingguy/2013/02/27/powertip-use-powershell-to-easily-find-how-long-a-process-runs/>

Use the New-TimeSpan cmdlet and specify the –Start parameter as the results from Get-Process on a process and the StartTime property. This is shown here using Notepad as an example:

```
PS C:\> New-TimeSpan -Start (get-process notepad).StartTime
```

Note: this method doesn't work well with every process.

GFlags

The Microsoft GFlags utility can be used to detect process stops or kills, however it must be setup to monitor a specific process in advance. Note: GFlags is a debugging utility and it may have some impact on performance.

<https://docs.microsoft.com/en-us/windows-hardware/drivers/debugger/gflags>

EE.9 Detect unusual/unauthorized attachment, insertion, and/or removal to/from processes (e.g. DLL injection)

Malware may attempt to hide its activities from antivirus software by attaching or inserting itself into a legitimate process and/or service (rather than creating its own process service). Reviewing the legitimate processes and/or services in detail could identify these possible malicious attachments or insertions. Use one or more of the methods below.

A. Handle (Microsoft SysInternals)

<https://docs.microsoft.com/en-us/sysinternals/downloads/handle>

This is a command line utility. It may be helpful to send the output to a text file for review. Look for unrecognized attachment/insertion to legitimate processes. Compare potentially targeted ICS applications or services to the baseline (see Enclosure E. FMC Baseline, section E.6, subsection b.2.e Handle).

handle >> output.txt

Example:

C:\temp>handle

```
Nthandle v4.11 - Handle viewer
Copyright (C) 1997-2017 Mark Russinovich
Sysinternals - www.sysinternals.com

-----
System pid: 4 \<unable to open process>
 4C: File (R--) C:\Program Files (x86)\Common Files\Antivirus
Shared\EENGINE\ANTIVIRUS.DAT
 58: File (R--) C:\Windows\System32\config\TxR\{00000000-0000-0000-0000-
000000000000}.TMContainer000000000000000000000001.regtrans-ms
 60: File (R--) C:\Windows\System32\config\TxR\{00000000-0000-0000-0000-
000000000000}.TMContainer000000000000000000000002.regtrans-ms
 80: File (RW-) \clfs
 84: File (---) C:\Windows\System32\config\RegBack\SYSTEM
 94: File (R--) C:\System Volume Information\EfaData\APPLICATION.DB
A4: File (RW-) \clfs
A8: File (RWD) \clfs
AC: File (RWD) \clfs
B0: File (RWD) C:\$Extend\$RmMetadata\$Txf
B4: File (R--) \clfs
B8: File (R--) 
C:\$Extend\$RmMetadata\$TxfLog\$TxfLogContainer000000000000000000000001
BC: File (R--) C:\$Extend\$RmMetadata\$TxfLog\$TxfLog.blf
C0: File (RWD) \clfs
C4: File (RWD) C:\Windows\System32\catroot\{00000000-0000-0000-0000-
000000000000}
```

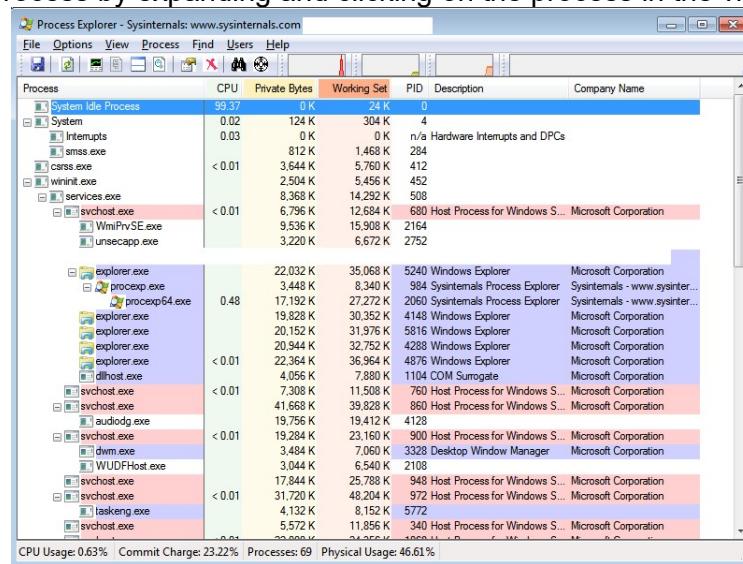
[snip]

B. Process Explorer (Microsoft SysInternals)

<https://docs.microsoft.com/en-us/sysinternals/downloads/process-explorer>

Process Explorer is the GUI based version of Handle. Compare potentially targeted ICS applications or services to the baseline (see Enclosure E. FMC Baseline, section E.6, subsection b.2.e Handle).

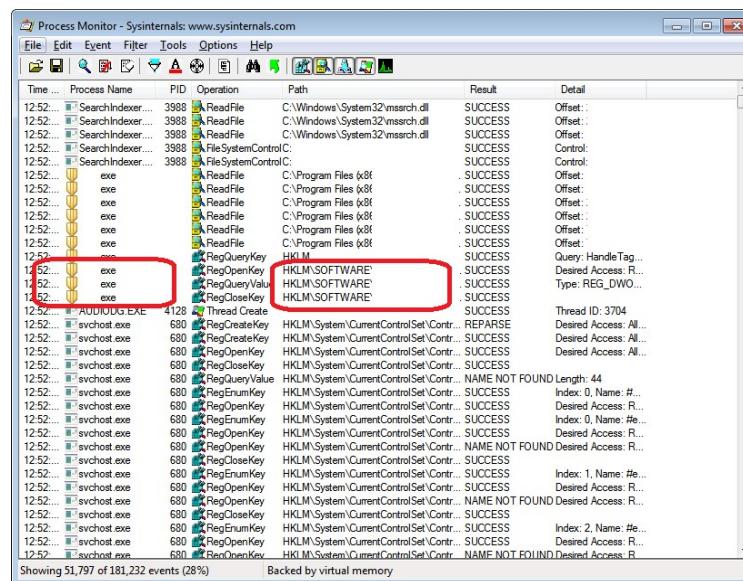
If time allows, also search for memory that is marked as RWX and review for clues of an executable file or injected code (Note however that this requires manually reviewing each process by expanding and clicking on the process in the viewer).



C. Process Monitor (Microsoft SysInternals)

<https://docs.microsoft.com/en-us/sysinternals/downloads/procmon>

Use Procmon GUI to monitor for unknown files (or manipulated paths); also review registry entries for unauthorized activity.



D. Monitor use of Regsvr32.exe (Windows)

Detect unauthorized use of regsvr32.exe to register or unregister DLLs in the Windows Registry. Consider logging/monitoring access to this file.
<https://technet.microsoft.com/en-us/library/bb490985.aspx>

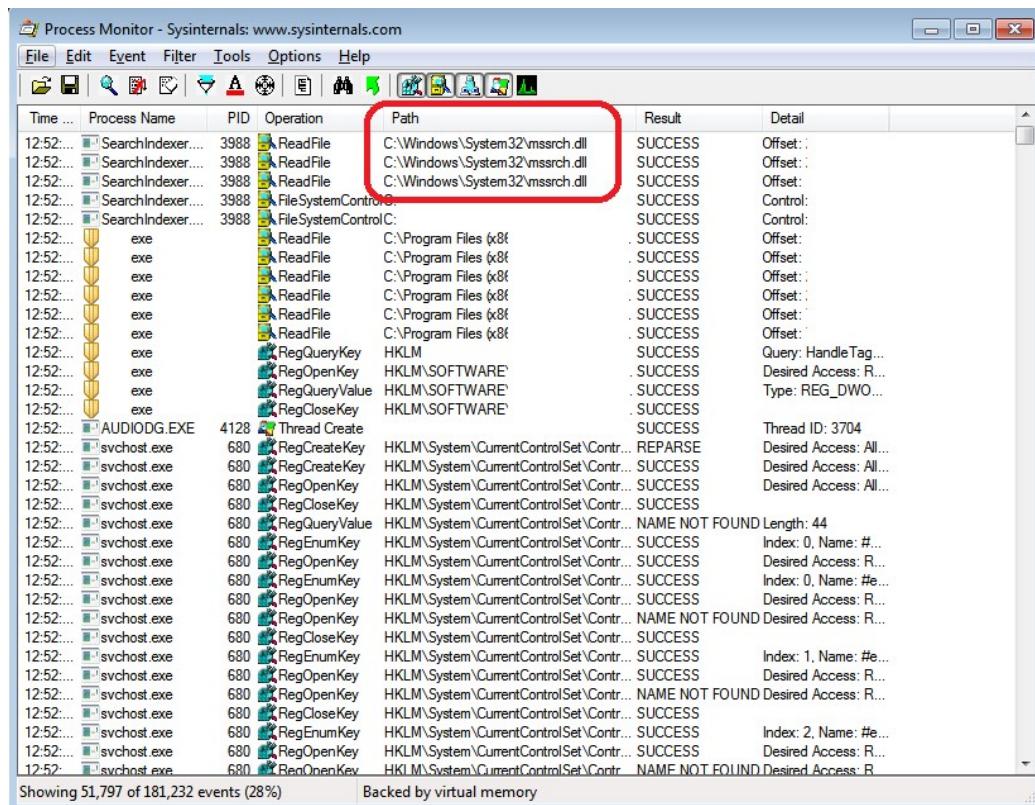
EE.10 Detect malware overwrite of an existing application or Windows service's "image path" (file location information)

Overwrite of the image path in the Windows Registry can be used to establish malware persistence. Malware may sometimes attempt to overwrite the image paths (file locations) of legitimate files in the Windows Registry in order to point to the location of a malicious file. In doing this, the malware may be able to redirect the OS (or user) to execute the malicious file instead of the legitimate one originally intended by the OS (or user). It is important to compare the **full image path** when performing this check.

In addition to the method shown in section D.5, subsection 29, two methods to review application or service image paths are listed below. Compare the paths of potentially targeted applications or services to the image paths recorded in the baseline (see Enclosure E. FMC Baseline, section E.6, subsection b.2.d Capture Services).

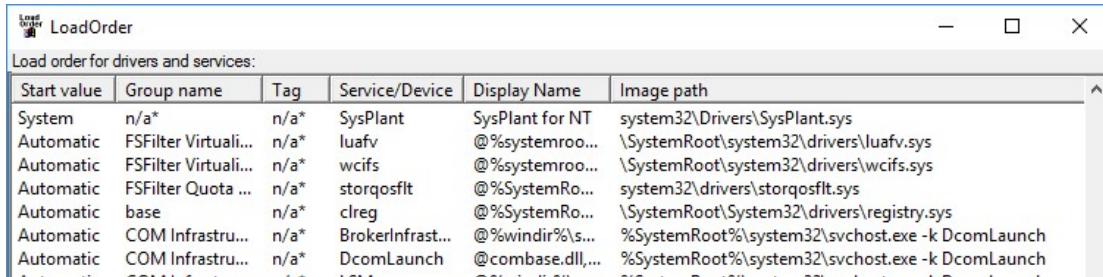
A. SysInternals [ProcMon](#) GUI can display image paths:

<https://docs.microsoft.com/en-us/sysinternals/downloads/procmon>



Time ...	Process Name	PID	Operation	Path	Result	Detail
12:52...	SearchIndexer....	3988	ReadFile	C:\Windows\System32\msrssch.dll	SUCCESS	Offset: ;
12:52...	SearchIndexer....	3988	ReadFile	C:\Windows\System32\msrssch.dll	SUCCESS	Offset: ;
12:52...	SearchIndexer....	3988	ReadFile	C:\Windows\System32\msrssch.dll	SUCCESS	Offset: ;
12:52...	SearchIndexer....	3988	File SystemControlC:		SUCCESS	Control: ;
12:52...	SearchIndexer....	3988	File SystemControlC:		SUCCESS	Control: ;
12:52...	exe		ReadFile	C:\Program Files\x86\	. SUCCESS	Offset: ;
12:52...	exe		ReadFile	C:\Program Files\x86\	. SUCCESS	Offset: ;
12:52...	exe		ReadFile	C:\Program Files\x86\	. SUCCESS	Offset: ;
12:52...	exe		ReadFile	C:\Program Files\x86\	. SUCCESS	Offset: ;
12:52...	exe		ReadFile	C:\Program Files\x86\	. SUCCESS	Offset: ;
12:52...	exe		ReadFile	C:\Program Files\x86\	. SUCCESS	Offset: ;
12:52...	exe		RegQueryKey	HKLM\	SUCCESS	Query: HandleTag...
12:52...	exe		RegOpenKey	HKLM\SOFTWARE\	. SUCCESS	Desired Access: R...
12:52...	exe		RegQueryValue	HKLM\SOFTWARE\	. SUCCESS	Type: REG_DWO...
12:52...	exe		RegCloseKey	HKLM\SOFTWARE\	. SUCCESS	
12:52...	AUDIODG.EXE	4128	Thread Create		SUCCESS	Thread ID: 3704
12:52...	svchost.exe	680	RegCreateKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: All...
12:52...	svchost.exe	680	RegCreateKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: All...
12:52...	svchost.exe	680	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: All...
12:52...	svchost.exe	680	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
12:52...	svchost.exe	680	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND Length: 44	
12:52...	svchost.exe	680	RegEnumKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Index: 0, Name: #...
12:52...	svchost.exe	680	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
12:52...	svchost.exe	680	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
12:52...	svchost.exe	680	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
12:52...	svchost.exe	680	RegEnumKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Index: 0, Name: #...
12:52...	svchost.exe	680	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
12:52...	svchost.exe	680	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND Desired Access: R...	
12:52...	svchost.exe	680	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
12:52...	svchost.exe	680	RegEnumKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Index: 1, Name: #...
12:52...	svchost.exe	680	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
12:52...	svchost.exe	680	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND Desired Access: R...	
12:52...	svchost.exe	680	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
12:52...	svchost.exe	680	RegEnumKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Index: 2, Name: #...
12:52...	svchost.exe	680	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
12:52...	svchost.exe	680	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND Desired Access: R...	

- B. SysInternals [LoadOrder](#) can show process image paths
<https://docs.microsoft.com/en-us/sysinternals/downloads/loadorder>



The screenshot shows a Windows application window titled "LoadOrder". The title bar has standard minimize, maximize, and close buttons. The main area is a table with the following columns: Start value, Group name, Tag, Service/Device, Display Name, and Image path. The data rows are as follows:

Start value	Group name	Tag	Service/Device	Display Name	Image path
System	n/a*	n/a*	SysPlant	SysPlant for NT	system32\Drivers\SysPlant.sys
Automatic	FSFilter Virtuali...	n/a*	luafv	@%systemroo...	\SystemRoot\system32\drivers\luafv.sys
Automatic	FSFilter Virtuali...	n/a*	wcifs	@%systemroo...	\SystemRoot\system32\drivers\wcifs.sys
Automatic	FSFilter Quota ...	n/a*	storqosflt	@%SystemRo...	system32\drivers\storqosflt.sys
Automatic	base	n/a*	creg	@%SystemRo...	\SystemRoot\System32\drivers\registry.sys
Automatic	COM Infrastru...	n/a*	BrokerInfrast...	@%windir%\s...	%SystemRoot%\system32\svchost.exe -k DcomLaunch
Automatic	COM Infrastru...	n/a*	DcomLaunch	@combase.dll,...	%SystemRoot%\system32\svchost.exe -k DcomLaunch

Search Order Hijacking

An additional method that malware may use to manipulate a legitimate executable or service is called Search Order Hijacking. In this method, the malware may modify the OS “Path” variable so that a malware’s folder location precedes the legitimate folder location. By manipulating the search path, the malware file will be called (rather than the legitimate file) when the OS or the user requests the legitimate file.

Check the Path Variable for malicious modification (and compare to baseline):

Windows 10 and Windows 8

1. Open Settings, System, About, System Info,
2. Click the Advanced system settings,
3. Click Environment Variables, System Variables, find the PATH environment variable and review it.

Windows 7

1. From the desktop, right click the Computer icon.
2. Choose Properties from the context menu.
3. Click the Advanced system settings link.
4. Click Environment Variables, System Variables, find the PATH environment variable and review it.

Unix/Linux

Bash Shell

Edit the startup file (~/.bashrc) to check the path

C Shell (csh)

Edit the startup file (~/.cshrc) to check the path

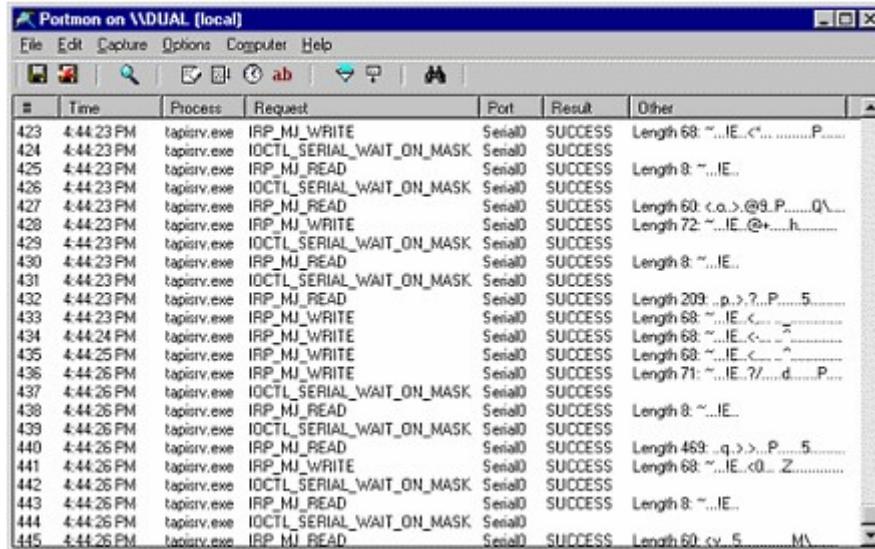
Alternately, malware may simply place a malicious file into an existing folder that precedes a legitimate folder in the path variable. To combat this scenario, it is important to specify the full path to the legitimate file when requesting a file.

EE.11 Detect malware manipulation of serial ports/connected serial devices

ICS focused malware may attempt to manipulate serial connections available on a target host (if found) in order to target connected ICS hardware. It may be beneficial to evaluate the configurations and status of a host's serial ports. The Windows' *mode* command (see Enclosure D, section D.5, step 30) is used to review these configurations and the user can then compare the configuration information to baseline. Additional utilities and commands listed below can also assist with review.

- Use Microsoft SysInternals [Process Explorer](#) utility to search for open handles (associated with serial ports).
<https://docs.microsoft.com/en-us/sysinternals/downloads/process-explorer>
 - Look for "device\serial"
 - Also consider USB to serial port converters, look for "device\vcp" (Virtual COM Port)
- Review the following Windows registry key:
HKEY_LOCAL_MACHINE\Hardware\DeviceMap\SerialComm
- Review output from following command:
wmic path Win32_SerialPort get DeviceID,Name
- Review output from chgport command:
e.g.:
C:\>chgport
COM3 = \Device\Serial0
- The SysInternals [Portmon](#) utility can log to a file (to facilitate logging/monitoring).
<https://docs.microsoft.com/en-us/sysinternals/downloads/portmon>

SysInternals Portmon



The screenshot shows the Portmon application interface with the title bar "Portmon on \DUAL (local)". The menu bar includes File, Edit, Capture, Options, Computer, and Help. Below the menu is a toolbar with icons for File, Edit, Capture, Options, Computer, Help, and a search function. The main window displays a table of network traffic logs. The columns are: #, Time, Process, Request, Port, Result, and Other. The table contains approximately 45 rows of data, each representing a network event. The "Request" column shows various API calls such as IRP_MJ_WRITE, IRP_MJ_READ, IOCTL_SERIAL_WAIT_ON_MASK, and others. The "Port" column consistently shows "Serial0". The "Result" column shows "SUCCESS" for most entries. The "Other" column displays hex dump representations of data transferred.

#	Time	Process	Request	Port	Result	Other
423	4:44:23 PM	taskmgr.exe	IRP_MJ_WRITE	Serial0	SUCCESS	Length 68: ^...IE.<.....P....
424	4:44:23 PM	taskmgr.exe	IOCTL_SERIAL_WAIT_ON_MASK	Serial0	SUCCESS	Length 8: ^...IE..
425	4:44:23 PM	taskmgr.exe	IRP_MJ_READ	Serial0	SUCCESS	Length 60: <...@.P.....0\....
426	4:44:23 PM	taskmgr.exe	IOCTL_SERIAL_WAIT_ON_MASK	Serial0	SUCCESS	Length 72: ^...IE.@+...h.....
427	4:44:23 PM	taskmgr.exe	IRP_MJ_READ	Serial0	SUCCESS	Length 8: ^...IE..
428	4:44:23 PM	taskmgr.exe	IRP_MJ_WRITE	Serial0	SUCCESS	Length 209: ..p,>?..P....5.....
429	4:44:23 PM	taskmgr.exe	IOCTL_SERIAL_WAIT_ON_MASK	Serial0	SUCCESS	Length 68: ^...IE.<...Z.....
430	4:44:23 PM	taskmgr.exe	IRP_MJ_READ	Serial0	SUCCESS	Length 68: ^...IE.<...Z.....
431	4:44:23 PM	taskmgr.exe	IOCTL_SERIAL_WAIT_ON_MASK	Serial0	SUCCESS	Length 8: ^...IE..
432	4:44:23 PM	taskmgr.exe	IRP_MJ_READ	Serial0	SUCCESS	Length 209: ..p,>?..P....5.....
433	4:44:23 PM	taskmgr.exe	IRP_MJ_WRITE	Serial0	SUCCESS	Length 68: ^...IE.<...Z.....
434	4:44:24 PM	taskmgr.exe	IRP_MJ_WRITE	Serial0	SUCCESS	Length 68: ^...IE.<...Z.....
435	4:44:25 PM	taskmgr.exe	IRP_MJ_WRITE	Serial0	SUCCESS	Length 68: ^...IE.<...Z.....
436	4:44:26 PM	taskmgr.exe	IRP_MJ_WRITE	Serial0	SUCCESS	Length 71: ^...IE.?...d....P....
437	4:44:26 PM	taskmgr.exe	IOCTL_SERIAL_WAIT_ON_MASK	Serial0	SUCCESS	Length 8: ^...IE..
438	4:44:26 PM	taskmgr.exe	IRP_MJ_READ	Serial0	SUCCESS	Length 469: ..q,>?..P....5.....
439	4:44:26 PM	taskmgr.exe	IOCTL_SERIAL_WAIT_ON_MASK	Serial0	SUCCESS	Length 68: ^...IE.<...Z.....
440	4:44:26 PM	taskmgr.exe	IRP_MJ_READ	Serial0	SUCCESS	Length 68: ^...IE.<...Z.....
441	4:44:26 PM	taskmgr.exe	IRP_MJ_WRITE	Serial0	SUCCESS	Length 469: ..q,>?..P....5.....
442	4:44:26 PM	taskmgr.exe	IOCTL_SERIAL_WAIT_ON_MASK	Serial0	SUCCESS	Length 68: ^...IE.<...Z.....
443	4:44:26 PM	taskmgr.exe	IRP_MJ_READ	Serial0	SUCCESS	Length 8: ^...IE..
444	4:44:26 PM	taskmgr.exe	IOCTL_SERIAL_WAIT_ON_MASK	Serial0	SUCCESS	Length 60: cv.5.....M\....
445	4:44:26 PM	taskmgr.exe	IRP_MJ_READ	Serial0	SUCCESS	Length 60: cv.5.....M\....

EE.12 Network Card - Promiscuous mode detection

Network cards in Promiscuous mode will attempt to “listen” to all traffic on the local subnet (rather than only the traffic intended for the host). Malware could possibly use this mode to gather sensitive information.

Linux methods:

- A. Run
ifconfig -a | grep PROMISC
- B. Run
ip link | grep PROMISC
- C. Detect presence of libpcap file
- D. Review logs (e.g. “eth0 entered promiscuous mode”)
/var/log
/var/log/audit

Windows methods:

- A. Via PowerShell:
c:\powershell
Get-NetAdapter | Format-List -Property ifAlias, PromiscuousMode
(Note: “Get-NetAdapter” is not available in Win7 → but works in Windows 10)
- B. Detect presence of winpcap
(detect wpcap.dll, \[Windows directory]\System32\Drivers\NPF.sys
or detect using msinfo32 utility, Software Environment, Drivers)
<https://www.winpcap.org/misc/faq.htm#Q-1>
or detect netcap.exe (Microsoft’s Net Monitor)
- C. **Promqry** Detection tool (requires Microsoft .NET)
<https://support.microsoft.com/en-us/help/892853/description-of-promqry-1-0-and-promqryui-1-0>
<http://www.microsoft.com/en-us/download/details.aspx?id=1851>
- D. Review Windows Security Event Log – EventID: 4688 with session: 0x3CC97

Network method:

Send a packet with the correct destination IP but an incorrect destination MAC to the host in question, if the host replies it is likely in promiscuous mode.

EE.13 Detect “Wiper” type malware activity

Detect malicious overwrite of ICS file types and/or configuration files. Review both local drives and mapped network drives for unexpected changes.

Note: Be sure to identify and review file-types associated with **your** environment's specific ICS products.

Some examples of ICS files/file types:

- *.scl
- *.cid
- *.scd
- *.paf

SYS_BASCON.COM

Review local system for malicious overwrite of Windows system, application, backup, or database files. Check one or more of the following traits:

- file hash
 - Using CertUtil (see Appendix E, section EE.2 for details)
 - Using SigCheck, (see Appendix E, section EE.15 for details)
- timestamp
- size

Some examples of files to review for changes:

- *.exe
- *.dll
- *.ini
- *.xml (note: may not be useful if application uses xml files for data, rather than configuration)

Backup and/or archive files. Backup files may require special consideration since files may frequently change (file hash and timestamp traits will likely not be useful). Just determine whether backup files are valid or corrupt.

Examples:

- *.zip
- *.7z
- *.tar
- *.rar
- *.bak
- *.bk
- *.bkp

Note: Database files will require special consideration since database files frequently change (file hash and timestamp traits will likely not be useful). Just determine if database files are valid or corrupt.

Examples:

- *.mdf (Microsoft SQL Server)
- *.ldf (Microsoft SQL Server)

EE.14 Detect unexpected encrypted or high entropy files

The Microsoft SysInternals [sigcheck](#) utility with the “-a” flag (“sigcheck -a”) can show the entropy level of a file to possibly identify encrypted files. Unexpected files with entropy ≥ 8 may warrant further review. Note: It is recommended to perform this check selectively on only unexpected or suspicious files (as unencrypted compressed files may cause false positives).

<https://docs.microsoft.com/en-us/sysinternals/downloads/sigcheck>
 Example (showing the entropy level of an AES256 encrypted zip file)

```
C:\temp>sigcheck -a mspaint-bad.zip

Sigcheck v2.60 - File version and signature viewer
Copyright (C) 2004-2017 Mark Russinovich
Sysinternals - www.sysinternals.com

C:\temp\mspaint-bad.zip:
Verified: Unsigned
File date: 12:11 PM 1/11/2018
Publisher: n/a
Company: n/a
Description: n/a
[...snip...]
Entropy: 8
```

EE.15 Malicious File Detection – via file hash

The Microsoft SysInternals [sigcheck](#) utility with the “-h” flag (“sigcheck -h”) can run a cryptographic hash of a file (e.g. md5, sha, etc). This can be used to compare a suspicious file against known bad files (i.e. either from reporting or from online services such as VirusTotal).

<https://docs.microsoft.com/en-us/sysinternals/downloads/sigcheck>
 Example:

```
C:\temp>sigcheck -h mspaint-bad.zip

Sigcheck v2.60 - File version and signature viewer
Copyright (C) 2004-2017 Mark Russinovich
Sysinternals - www.sysinternals.com

C:\temp\mspaint-bad.zip:
Verified: Unsigned
File date: 12:11 PM 1/11/2018
Publisher: n/a
Company: n/a
Description: n/a
[...snip...]
MD5: 6F4E82C9BBDA8B7D6D8B88CB586D416
SHA1: 794CDF180C96AAE6A483F7F750B873A8718326A3
PESHA1: 794CDF180C96AAE6A483F7F750B873A8718326A3
PE256:
6EB33BF60C360E4B9Dacfad106148D1FF1CEC45258460FA38FD9B799A6F6D8C6
SHA256:
6EB33BF60C360E4B9Dacfad106148D1FF1CEC45258460FA38FD9B799A6F6D8C6
```

EE.16 Detect Privilege escalation

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

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

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

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

- B. Review accounts and permissions to detect unauthorized additions to privileged groups/accounts:

Run wmic useraccount list full to display a list of users on the local machine and compare output to the baseline generated in Enclosure E FMC Baseline, section E.6, subsection b.2.f.

e.g.

```
C:\temp>wmic useraccount list full

AccountType=512
Description=Local Built-In Administrator Account
Disabled=TRUE
Domain=PC
FullName=Administrator
InstallDate=
LocalAccount=TRUE
Lockout=FALSE
Name=Administrator
PasswordChangeable=TRUE
PasswordExpires=TRUE
PasswordRequired=TRUE
SID=S-1-5-21-0000000000-0000000000-00000000-0000
SIDType=1
...[snip]...
```

EE.17 Detect unauthorized usage Windows admin tools/utilities

Malware may attempt to use administrative or system utilities in order to execute tasks or gather information. Monitor for unauthorized use of these utilities.

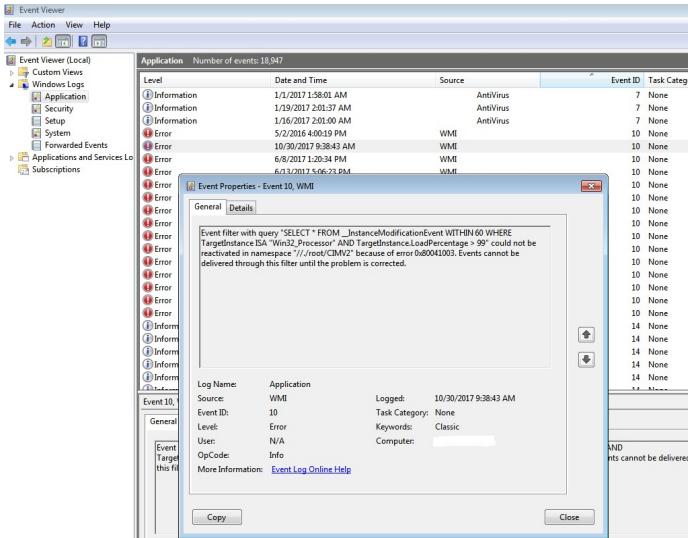
A. PowerShell

Review Windows event log for evidence of unexpected PowerShell / WMI activity.

Detect eventID 10 (in Application Event log)

source = WMI

Example:



More comprehensive PowerShell Logging is configured through Group Policy ...:

Administrative Templates -> Windows Components -> Windows PowerShell

...and registry changes::

Script Block Logging:

HKLM\SOFTWARE\Wow6432Node\Policies\Microsoft\Windows\PowerShell\ScriptBlock
Logging ? EnableScriptBlockLogging = 1

Transcription: (By default, transcripts are written to the user's documents folder)

HKLM\SOFTWARE\Wow6432Node\Policies\Microsoft\Windows\PowerShell\Transcriptio
n ? EnableTranscripting = 1

HKLM\SOFTWARE\Wow6432Node\Policies\Microsoft\Windows\PowerShell\Transcriptio
n ? EnableInvocationHeader = 1

HKLM\SOFTWARE\Wow6432Node\Policies\Microsoft\Windows\PowerShell\Transcriptio
n ? OutputDirectory = "" (Enter path. Empty = default)

Review eventIDs 400, 403, 4104, 7937, 32850, 32867, 32868, 40961

(in PowerShell Event log). Check the details tab for additional information.

source = Powershell

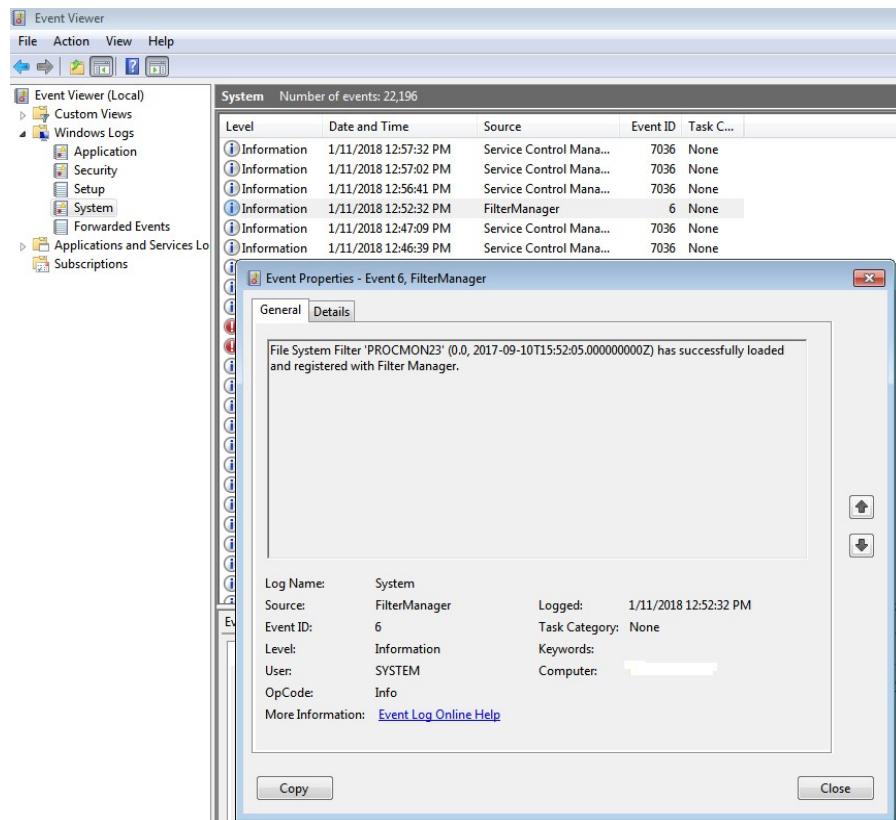
B. SysInternals

Review Windows event log for evidence of unexpected use of SysInternals utilities. For additional information on SysInternals utilities, see Appendix E, section EE.0.

Detect eventID 6 (in System Event log)

Example for Process Monitor:

"File System filter 'procmon23'...has successfully loaded..."



Detect PsExec service installation or usage via Windows Event log:

Review Event ID 7045 (in SYSTEM Event Log) for service/process name = PSEXESVC

Review Event ID 7035 (in SYSTEM Event Log) for description "The PsExec service was successfully sent a start control."

Review Event ID 7036 (in SYSTEM Event Log) for description "The PsExec service entered the running state."