Risk Assessments, Continuous Monitoring & Intrusion Detection, Incident Response

Michael Chipley, PhD PMP LEED AP
President

January 6, 2014

mchipley@pmcgroup.biz
Risk Assessments

Multiple Standards and Tools For Conducting Cyber Risk Assessments
• DHS CSET
• SANS Top 20 Controls
• ISA
• GSA FedRamp
• Kali Linux
• SamuraiFTSU
• Gleg
• Wireshark

Risk Assessment model based on:
• NIST SP 800-53 Rev 4
• NIST SP 800-82 Rev 1, Rev in Spring 2014
SANS Twenty Critical Security Controls

http://www.sans.org/critical-security-controls/

http://www.sans.org/critical-security-controls/
ISA Security for Industrial Control Systems

http://www.isa.org/Template.cfm?Section=Standards2&template=/Ecommerce/ProductDisplay.cfm&ProductID=13420
GSA FedRamp

http://www.gsa.gov/portal/category/102371
4. SECURITY ASSESSMENT RESULTS

This section describes all security weaknesses found during testing. The following elements for each security weakness are reported.

- Identifier
- Name
- Source of Discovery
- Description
- Affected IP Address/Hostname/Database
- Source
- Applicable Threats
- Likelihood
- Impact
- Risk Statement
- Risk Exposure
- Recommendation
DoD ICS Overlay and RMF Implementation

ICS Overlay v1, v2
Began in 2013
Use CSET Tool

Step 1: CATEGORIZE System
- Categorize the system in accordance with CNSSI 1253
- Initiate the Security Plan (SP)
- Register system with DoD Component IA Program
- Assign qualified personnel to RMF roles

Step 2: SELECT Security Controls
- Common Control Identification
- Select security controls and document SP
- Develop system-level continuous monitoring strategy
- Review and approve SP and continuous monitoring strategy

Step 3: IMPLEMENT Security Controls
- Implement control solutions consistent with DoD and Component IA architectures
- Document security control implementation in SP

Step 4: ASSESS Security Controls
- Develop and approve Security Assessment Plan
- Assess security controls
- SCA prepares Security Assessment Report (SAR)
- Conduct initial remediation actions

Step 5: AUTHORIZE System
- Prepare the POA&M
- Submit Security Authorization Package (SP, SAR and POA&M) to AO
- AO conducts final risk determination
- AO makes authorization decision

Step 6: MONITOR Security Controls
- Determine impact of changes to the system and environment
- Assess selected controls annually
- Conduct needed remediation
- Update SP, SAR and POA&M
- Report security status to AO
- AO reviews reported status
- Implement system decommissioning strategy

IT RMF Model Can be Readily Adopted for ICS RMF

Initial ATO’s 2014?
2015?
CSET Resource Library

This library of cyber security standards, reports, and templates are provided for your convenience. Additionally, there are several cyber security guides and white papers to assist you in gaining a general background in cyber security, determining priorities, or specific help. Specific helps include white papers and instructions on securing network components such as a firewall or web server.

Library documents may be browsed using the "Document Tree" tab on the left side of the screen. Documents are grouped by type and topic. If you are looking for a specific document, a keyword or title search may also be performed using the "Search" tab in the left pane. Clicking on a document title link in the left-hand pane displays the document. To save a document to your local hard drive click the export button.
CSET Step 1 Assessment Mode

[Image of CSET Step 1 Assessment Mode interface]

Most users should select the 'Questions Based' option for a comprehensive evaluation based on questions rather than requirements.

To see the exact requirements for a specific standard, choose the 'Standard Requirements Based' option. This would be common for regulated sectors where the precise wording is important.

What approach would you like to take to perform a cyber security evaluation?
- Questions Based
- Standard Requirements Based

STEP 2 - Questions and Standards

STEP 3 - Security Assurance Level (SAL)
CSET Step 2 Questions and Standards

STEP 2 - Questions and Standards

General Control System Standards:
- Universal Questions
- Key Questions
- NIST Special Publication 800-82
- NIST Special Publication 800-53 Rev 3 App I

Sector Specific Standards:
- CFATS Risk-Based Performance Standards Guide 8 - Cyber
- NERC CIP-002 through CIP-009 Rev 3
- NERC CIP-002 through CIP-009 Rev 4
- NRC Regulatory Guide 6.71
- TSA Pipeline Security Guidelines April 2011

Information Technology (IT) Specific Standards:
- NIST Special Publication 800-53 Rev 3
- NIST Special Publication 800-53 Rev 4

Requirements Mode Only Standards:
- Catalog Of Recommendations Rev 7
- Consensus Audit Guidelines (CAG)
- Committee on National Security Systems Instruction (CNSSI) 1253
- CNSSI No. 1253 Baseline
- CNSSI No. 1253 Industrial Control System (ICS) Overlay
- DOD Instruction 8500.2

Confidentiality Level:
- Classified
- Sensitive
- Public

MAC Level:
- MAC I
- MAC II
- MAC III
CSET Step 3 Security Assurance Level
CSET Architecture Diagram
CSET Controls Questions

Complete Family, Control, Supplemental, Enhancements, Parameter, Regulatory Sections
CSET Dashboard
CSET Reports
Continuous Monitoring & Intrusion Detection

Continuous Monitoring is Step 6 of the RMF

- IT systems
- OT systems

CM Tools

- DHS CM Program
- Sophia
- Vendors (McAfee, Symantec, Tofino, Industrial Defender, etc.)
Organizations take the following steps to establish, implement, and maintain Information Security Continuous Monitoring (ISCM):

- **Define** an ISCM strategy;
- **Establish** an ISCM program;
- **Implement** an ISCM program;
- **Analyze** data and **Report** findings;
- **Respond** to findings; and
- **Review and Update** the ISCM strategy and program.
Continuous Diagnostics and Mitigation (CDM) Program Tools and Continuous Monitoring as a Service (CMaaS) Blanket Purchase Agreements (BPAs)

The General Services Administration (GSA), Federal Acquisition Service (FAS), Assisted Acquisition Services (AAS), Federal Systems Integration and Management Center (FISMA), the FBI, and the Office of Cybersecurity and Communications (CSAC) offer a comprehensive cybersecurity solution for federal agencies. The CDM Program helps transform the way federal and other government entities manage their cyber networks through strategically sourced tools and services and enhances the ability of government entities to strengthen the posture of their cyber networks. The CDM Program brings an enterprise approach to continuous diagnostics, and allows consistent application of best practices.

- Ordering
- Overview
- Facts and features

Ordering

The most recent version of the Ordering Guide, which includes eligibility requirements and BPA holder POCs, can be found here (PDF, 679 KB).

The CDM Toolset/CMAaaS BPAs were established using GSA Multiple Award IT Schedule 71 pricing as a benchmark to establish the initial discounts for the BPAs, as well as tiered discounts based on cumulative quantities. A Federal Strategic Sourcing Initiative (FSSI) type reporting mechanism was built into the BPAs, with quarterly reporting of sales to track usage, and to ensure volume discounts are achieved by all users of the BPAs over the life of the program. The BPAs were established with broad accessibility, to allow for greater usage to achieve better pricing and greater discounts.

http://www.gsa.gov/portal/content/176671?utm_source=FAS&utm_medium=print-radio&utm_term=cdm&utm_campaign=shortcuts
IT Versus OT Continuous Monitoring

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

Intrusion Detection Systems (Passive)
- PLC, RTU, Sensor Modbus, LonTalk, BACNet, DNP 3
Sophia Passive Monitoring of Control Systems

http://nexdefense.com/about-sophia/how-does-it-work/
DHS ICS-CERT Common Vulnerabilities

Figure 1. Categories of vulnerabilities identified in 2009–2010 CSSP product assessments.

- 47% Improper Input Validation
- 18% Permissions, Privileges, and Access Controls
- 11% Improper Authentication
- 8% Insufficient Verification of Data Authenticity
- 8% Indicator of Poor Code Quality
- 5% Security Configuration and Maintenance
- 3% Credentials Management

Figure 4. CSSP assessment findings and ICS-CERT vulnerability disclosures per ICS component type.
Key Signs You Are Compromised

1. Look at number of highest IP address out of your network
2. Look at longest number of connections
3. Look at where most data is being sent
4. Look at percent of traffic out (filter for Cloud based services)
5. Look for new IP addresses never connected before

- Building control systems typically transmit data to the Human Machine Interface, Historian and other sensors, and typically don’t need to connect to other outside IP address's (except for remote maintainence)
- Advanced Meter Infrastructure (AMI) and other “Smart” devices DO need two way communication, encrypt data

The Internet of Everything and IPV6 will connect billions of devices and sensors at every level.

Control Systems are becoming Cyber-Physical Systems, they will be compromised, malware specifically targeting these systems
CSET Incident Guidance

Recommended Practice:
Developing an Industrial Control Systems Cybersecurity Incident Response Capability

October 2009
Incidents: NIST SP 800-61 Rev 2

CSET Incident Response Plan Templates
SANS Incident Handling and Suspicious Events

1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Lessons Learned


http://pen-testing.sans.org/resources/downloads
CSET SANS Incident Identification Template
Control Systems Key Concepts

- Control systems are good candidates for Whitelisting
- Eliminate direct facing internet connections, route through an Operations Center with CM and IDS
- Keep backup software down to the device level firmware
- Complete a CSET Evaluation
- Prepare a Security Assessment Report
- Prepare a Systems Security Plan
- Prepare a CONOPS Plan
- Prepare an Incident Response Plan

Inbound Protection, Outbound Detection