Cybersecuring DoD Industrial Control Systems One Year Later…. 

Michael Chipley, PhD GICSP PMP LEED AP President 

February 23, 2015 

mchipley@pmcgroup.biz
Overview

- DoD CIO C&A Transformation
- NIST SP 800-53 and SP 800-82, CNSSI 1253
- DHS Cybersecurity Evaluation Tool (CSET)
- DoD RMF KS ICS PIT website
- eMASS with ICS PIT Step-By Step Manual Method
- Continuous Monitoring, Alerts and Advisories
- DHS Interagency Security Committee Converged Systems
- Cyber Workforce Skills and Credentials, Ranges
- Acquisition/Procurement
- Vendor Outreach and Meetings
- Cybersecuring ICS and BCS Workshops
DoDI 8500.01 and 8510.01 Update

Evoluted into the Joint Task Force Transformation Initiative Interagency Working Group (DoD, ODNI, NIST and CNSS), ongoing effort to produce a unified information security framework for the federal government.

Used existing NIST Special Publications as basis for developing Joint Transformation core documents.

DIACAP
Began as the IC Transformation effort to standardize C&A in the IC and to address reciprocity with DoD.

JTF

Revised 8500 Series
DoD is currently revising DoDD 8500.01, DoDI 8500.02, and DoDI 8510.01 to align with NIST Joint Task Force documents.

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

- Huge Cost Savings
  - No more planes and choppers cluttering up the deck
  - Less fuel used
- Noise Complaints way down
- Morale way up
- Drives over 400 yards with the wind
Standards - NIST 800-82 FPD 2015

Computer Security Division
Computer Security Resource Center

Computer Security Resource Center (CSRC)

The Computer Security Division’s (CSD) Computer Security Resource Center (CSRC) facilitates broad sharing of information security tools and practices, provides a resource for information security standards and guidelines, and identifies key security web resources to support users in industry, government, and academia.

CSRC is the primary gateway for gaining access to NIST computer security publications, standards, and guidelines plus other useful security-related information.

News

February 9, 2015
NIST announces the final public draft release of Special Publication 800-82, Revision 2, Guide to Industrial Control System (ICS) Security

January 29, 2015
Errata Update for Special Publication 800-53, Revision 4

Comments Due 10 March

Standards — NIST 800-82 FPD 2015

Computer Security Division
Computer Security Resource Center

Useful Resources
• 2013 CSD Annual Report
• A-Z List of Projects
• Cryptographic Toolkit
• FISMA Implementation Project
• National Vulnerability Database (NVD)
While many of controls in Appendix F of NIST SP 800-53 are applicable to ICS as written, many controls did require ICS-specific interpretation and/or augmentation by adding one or more of the following to the control…

An ICS overlay, which includes this ICS-specific guidance, is included in Appendix G of this document. Section 6 of this document also provides initial guidance on how 800-53 security controls apply to ICS. Initial recommendations and guidance, if available, are provided in an outlined box for each section.

In process of submitting to the CNSS the Appendix G ICS Overlay for adoption/approval

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

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

Protocols/Ports and Services
- Modbus: Master/Slave - Port 502
- BACnet: Master/Slave - Port 47808
- LonWorks/LonTalk: Peer to Peer - Port 1679
- DNP3: Master/Slave - Port 20000
- IEEE 802.x - Peer to Peer
- Zigbee - Peer to Peer
- Bluetooth – Master/Slave

Additional DoD content accepted and incorporated into the Final Public Release – “Industrial” is not the most desirable term, but it will work

http://csrc.nist.gov/
NIST SP 800-82 R2 Key Security Controls

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

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

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

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

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

Inbound Protection, Outbound Detection
DHS Cyber Security Evaluation Tool (CSET)

CSET 6.2 release has new DoD, CNSS, NIST and DHS references, control system dropdown lists

DoD Moving to Standardized Assessments via CSET
CSET 6.2 with CNSS RMF Supported

SAL as required by CNSSI 1253, NIST SP 800-60 Vol 2 Data Types
CSET 6.2 CNSS SAL C-I-A and Info Types

C-I-A Data Categorization with Special Factors Justification
CSET 6.2 Diagram Tool Enhancements

Additional Components, Building Control System template...more to come!
DoDI 8510.01 “Risk Management Framework for DoD IT”
- Provides clarity regarding what IT should undergo the RMF process and how

**AA = Full 6 steps of RMF, A = 4 steps of RMF**
(b) Examples of platforms that may include PIT are: weapons systems, training simulators, diagnostic test and maintenance equipment, calibration equipment, equipment used in the research and development of weapons systems, medical devices and health information technologies, vehicles and alternative fueled vehicles (e.g., electric, bio-fuel, Liquid Natural Gas that contain car-computers), buildings and their associated control systems (building automation systems or building management systems, energy management system, fire and life safety, physical security, elevators, etc.), utility distribution systems (such as electric, water, waste water, natural gas and steam), telecommunications systems designed specifically for industrial control systems including supervisory control and data acquisition, direct digital control, programmable logic controllers, other control devices and advanced metering or sub-metering, including associated data transport mechanisms (e.g., data links, dedicated networks).

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

RMF Knowledge Service > RMF General > IT > Industrial Control Systems

Industrial Control Systems Platform IT (PIT)

Background

DoDI 8500.01 and DoDI 8510.01 incorporate PIT and PIT systems into the Risk Management Framework (RMF) process. PIT may consist of both hardware and software that is physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems (i.e., platforms). PIT differs from products in that it is integral to a specific platform type as opposed to being used independently, or to support a range of capabilities (e.g., major applications, enclaves or PIT systems).

An Industrial Control System (ICS) is a specific type of PIT. An ICS consists of combinations of control components (e.g., electrical, mechanical, hydraulic, pneumatic) that act together to achieve an objective (e.g., transport matter or energy, maintain a secure and comfortable work environment, etc.). As defined by the National Institute of Standards and Technology (NIST), ICS is a general term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as the Programmable Logic Controllers (PLC) often found in the industrial sectors and critical infrastructures. For the DoD installations and Environment (I&E) community, ICS is used in its broadest sense to include all types of control systems (SCADA, DCS, building,

Key Documents and Tools

- ICS PIT Master List (Excel)
- ICS Overview
- NIST SP 800-82 R2 Industrial Control Systems Security Guide
- NIST SP 800-82 R2 Security Controls (Excel)
- NIST SP 800-53 R4 and NIST SP 800-82 R2 Merged
- DHS Cyber Security Tool (CSET)

RMF KS ICS PIT website planned released DoD wide Mar 2015

eMASS

- eMASS updated to include the RMF process
  - BEI created ICS PIT RMF Knowledge Service web page with instructions for:
    - registering ICS in eMASS
    - NIST SP 800-53 / 800-82 security controls to assess and authorize systems
  - BEI conducting test cases for various ICS system types, selecting appropriate controls (ICS “master list”, C-I-A matrix using NIST SP 800-60 data categorization)
    - FA4819-ICS-UMCS-NI-A = Utility Monitoring Control Systems [Electrical, Building Automation Systems]-No Interconnect-Assess
  - BEI conducting eMASS training/demos for EI&E community
    - 0800-0900 Overview of DoDI 8500/8510 RMF & PIT ICS, NIST Standards, ICS Protocols
    - 0900-0930 Overview of Shodan, Kali Linux, Samurai STFU, Wireshark
    - 0930 -1000 Using Shodan to Footprint ICS
    - 1000-1015 Break
    - 1015-1200 Using CSET: SAL, Network Arch Diagram, Inventory, Templates, Security Controls Evaluation, Reports, Data Aggregation & Trending, System Security Plan
    - 1200-1300 Working Lunch: SamuraiSTFU Modbus Pal, Wireshark Packet Captures
    - 1300-1400 Using eMASS; demonstration
    - 1400-1430 Using the Interim Excel files for uploading into eMASS
    - 1430-1500 Wrap Up Q&A
**Register PE = 1.5 hours, each additional system 0.5 hours**
CSET and eMASS Relationship

**System**
- eMASS (ATO and IATT)
  - DIACAP
  - RMF
  - Inheritance
  - Controls
  - AO Package

**DITPR**
- Component Registry
  - (APMS, DADMS, EITDR, DHP SIRT)

**MILCON / SRM**
- Security
- Medical
- Logistics
- Weapons

**XML Import/Export**

**CSET Tool**
- System List
- Network Diagram
- Inventory
- SSP Artifacts

**Real Property Control System Acquisition**
- 90% Design CSET
- 50-95% Construction FAT
- 100% Construction SAT
- Pen Test
- CSET Final

**Existing / Legacy Systems**
- Passive Monitoring Tools
  - Nessus
  - McAfee
  - Sophia
  - Grass Marlin

**Pen Test**
-**Inheritance Controls**
-**AO Package**
-**IT Enclave / IS PIT System**
-**PIT Service**
-**Security**
-**Medical**
-**Logistics**
-**Weapons**
CM, Alerts and Advisories

- **ICSA-14-105-03A** Siemens Industrial Products OpenSSL Heartbleed Vulnerability
  - Mitigation details for OpenSSL vulnerability in several Siemens industrial products

- **ICSA-14-175-01** Honeywell Falcon (XLWeb Linux/Webserver)
  - Allows anyone (without username or password) to log in as a system administrator
  - Known for months; multiple unpatched systems remain exposed to the Internet

- **ICSA-14-281-01A** Sophisticated Malware Campaign Compromising ICS
  - Targeted HMI products: GE Cimplicity, Advantech/Broadwin WebAccess, and Siemens WinCC; variant of BlackEnergy malware - automated tools to discover and compromise vulnerable systems

Who Reviews Alerts & Mitigates…Facility Engineers or IA SMEs?
ICS Monitoring and Network Attack Points

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

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

Client Side Attacks
Server Side Attacks
Network Attacks
Hardware Attacks
CSET 6.2 Grass Marlin Plug

Working with other products to get Visio import templates
Sophia Installs/Pilots

USMC – Recruit Depot, San Diego
Monitoring control systems networks for base facilities along with IT network that it is connected to

Naval Surface Warfare (NSWCCD) – Philadelphia
Begin pilot testing for intrusion detection capabilities for control system networks on board vessels
Testing in conjunction with two other complimentary technologies also developed at government labs

CYBERCOM
Installing for test and evaluation on 2/20

Working with CIO to define rules for HBSS and other passive IDS boundaries
Technological advances in system components, coupled with the interconnection capability, moved from Recommended Standards technology (e.g., RS-232, RS-422, RS-485, etc.) to Internet Protocol (IP) telecommunications standards (e.g., IPv6). Employing state-of-the-art systems, today’s security professional relies heavily upon IT infrastructure to host and interconnect the various components of a VMS, IDS, and PACS. Employing IT infrastructure to interconnect Electronic Security System (ESS) components across local area networks (LAN), wide area networks (WAN), metropolitan area networks (MAN) or the Internet requires a convergence between the traditional security community (operational management), and the IT community (enabler).

Moving to a universe of Converged Systems and IoT; ICS, Weapons, Medical..
Example: Navy Converged Systems

Innovative solution to offset the DoD Sequestration budget cuts!
Preliminary Converged Systems Approach

DITPR ICS PIT Guidance and Relationship to ICS PIT in eMASS

Some ICS are hybrid between PIT ICS (controls, sensors and devices) and a Defense Business System and need to be maintained in both DITPR and eMASS. Examples include:

- Access control/alarm systems that use badges/CAC for keyless entry (PII)
- Keyless entry/keypad systems (PII)
- Meter data management systems that combine head-end consumption data with back-end energy controllers (PCII, PII)
- Patient Monitoring Systems (PII, HIPPA)
- Vehicle Fueling/Charging Stations/Pumps (PCI)

These hybrid systems are categorized as "Converged Systems". (Reference the DHS ISC CVS White Paper). For converged systems, identify them as WMA or DBS and follow flow chart scenarios 3, 4, 5 or 6 to identify other systems that will need additional detail (SNAP-IT, Certified Funds, etc.). In the DITPR System Description, at the beginning of the Description enter, "This is a Converged IS and ICS PIT System."

As more converged systems become interconnected, the distinction between what is IS and what is ICS PIT becomes even more challenging. Contact Tracy DeBusk (Tracy.l.DeBusk.ctr@mail.mil) for assistance with DITPR and eMASS ICS PIT questions.

Use BOTH the NIST SP 800-53 R4 AND the NIST SP 800-82 R2 controls
i. **Cybersecurity Workforce**

(1) Cybersecurity workforce functions must be identified and managed, and personnel performing cybersecurity functions will be appropriately screened in accordance with this instruction and DoD 5200.2-R (Reference (t)), and qualified in accordance with DoDD 8570.01
Collect and Analyze Data
Capture cybersecurity workforce and training data to understand capabilities and needs.

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

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

Engage
Educate and energize all cybersecurity workforces and the American public to strengthen the nation’s front lines of cybersecurity.
Workforce Challenges
Workforce Cyber Skills – ICS PIT

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

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

Securely Provision
- Information Assurance (IA) Compliance
- Software Assurance and Security Engineering
- Systems Security Architecture
- Technology Research and Development
- Systems Requirements Planning
- Test and Evaluation
- Systems Development
DoD Cyber Ranges Work Group

JMETC Connectivity
- Functional Sites: 77
- New Sites Planned: 10
- Connection Points to Other Networks: 7

- Dedicated, trusted connectivity on SDREN (part of the GIG)
- Encrypted for Secret – System High
- DISA-registered IP address space
- Active monitoring of network performance
- Capable of supporting multiple simultaneous test events

Sites in Alaska
- Ft. Greely: CRT/2

Sites in Hawaii
- PEAR: 11th 105
- MNHCC

As of 17 Nov 2014

Chart showing trend from FY07 to FY14
ICS Cyber Ranges

You are here: Ranges >> Muscatacuck Urban Training Center >> MUTC Overview

**MUTC Overview**

“Camp Atterbury and Muscatacuck are great facilities. There’s no place like Muscatacuck, frankly, in the entire United States.”

–Maj. Gen. Jeffrey A. Jacobs, Commander USACAPOC(A)

*Spring 2013 issue of “Peacemaker”*

The Official Magazine of The U.S. Army Civil Affairs & Psychological Operations Command (Airborne)

**Communications/Technology**

- Cyber capabilities
- JTEN 2.0 Extensive fiber network
- VBS2 simulation environment
- After Action Review Facility with playback capability
- Range Operations Center communications
- Personnel and vehicle tracking technology
- Extensive telephone, cyber, and communication network capabilities
- Power lines and transformers of various types and designs used throughout the site
Acquisition Reform

Six reform recommendations:

1. Institute baseline cybersecurity requirements as a condition of contract award for appropriate acquisitions
2. Include cybersecurity in acquisition training
3. Develop common cybersecurity definitions for federal acquisitions
4. Institute a federal acquisition cyber risk management strategy
5. Include a requirement to purchase from original equipment manufacturers, their authorized resellers, or other trusted sources
6. Increase government accountability for cyber risk management

http://www.gsa.gov/portal/content/176547
Order Cybersecurity Risk Management Plan (OCRMP) Submittal, Review, and Acceptance

(1) Submittal.
(i) When submitting a proposal in response to any task order solicitation, Contractor shall submit its approved CCRMP to the ordering contracting officer as an addendum to the proposal.
(ii) If required by the task order solicitation, Contractor shall also provide an Order Cybersecurity Risk Management Plan (OCRMP) that includes additional information to address the specific security requirements of the task order solicitation.

Order Cybersecurity Risk Management Plan Update, Review, and Acceptance

(1) Updates.
(i) Contractor may update its OCRMP at any time after order award to ensure the Government is adequately assured of Contractor’s continuous ability to provide appropriate cybersecurity in the deliverables it provides under the contract.

CCRMP based on NIST SP 800-53 R4, or can use SANS Top 20 Arlington Workshops: "How To" Workshop: Develop a Contract Cybersecurity Risk Management Plan
Initially likely to pay a premium, then becomes industry standard
LEED is a good corollary, took a few years….but now a green is gold
FFC is hosting a half-day workshop on March XX 2015 focused on generating awareness of cyber security vulnerabilities, current and forthcoming guidance and protection strategies relevant to federal facility stakeholders.

Agenda:

0800 - 0815  Introductions, Purpose, Expected Outcome  (FFC Cameron Oskvig)
0815 - 0900  Facility control systems Vulnerability, Alert and Advisories Overview  
(OSD Daryl Haegley / ODNI Dave Retland)
0900 - 0930  Exploiting controls systems demonstration using Shodan, DB Exploit, 
Google Hacking, Diggity, Kali Linux  (OSD Michael Chipley)
0930 - 0945  Break
1015 - 1045  NIST SP 800-82 Industrial Control Systems Security Guide R2 (NIST Keith 
Stouffer)
1045 - 1130  DHS ICS-CERT and DHS Cyber Security Evaluation Tool (CSET) 
demonstration (INL Barry Hanson)
1130 - 1200  GSA / DoD control systems Cyber Policy and Strategy (GSA Josh Mordin / 
OSD Daryl Haegley)
ICS and BCS Cybersecurity Workshops 2

- 0800-0900 Overview of DoDI 8500/8510 RMF and PIT ICS, NIST Standards & Drivers, ICS Protocols
- 0900-0930 Overview of Shodan, Kali Linux, Samurai STFU, Wireshark
- 0930 -1000 Using Shodan to Footprint ICS
- 1000-1015 Break
- 1015-1200 Using CSET: SAL, Network Arch Diagram, Inventory, Templates, Security Controls Evaluation, Reports, Data Aggregation & Trending, System Security Plan
- 1200-1300 Working Lunch: SamuraiSTFU Modbus Pal, Wireshark Packet Captures
- 1300-1400 Using eMASS; demonstration
- 1400-1430 Using the Interim Excel files for uploading into eMASS
- 1430-1500 Wrap Up Q&A
SANS Control Systems Poster 2013

DoD Reference Architecture 2012

Coincidence?
DoD ICS Systems 2012

ICS Operations Center

Test and Development Environment

Tools
- Kali Linux
- SamuraiSTFU
- CSET
- Shodan

Internet

NOC

Network Operations Center

ICS PIT

Airfield Lighting

Buildings

Electrical

Natural Gas

Pier

POL

Rail

Steam

Traffic Management System

Water

Waste Water
Coincidence?!
If history holds any indication……

We said we need Model Ops Centers,
We need to address all Control Systems,
We need to see the whole picture,
We need the culture to change…..
Navy Shore Operations Concept

- Quality of Life
- Operations / Ops Support
- Facility Management
- Public Safety
- Enablers
- Logistics
- USW / Strike
- Strike Operations / C2
- AAW / BMD
- ASW / AAW

Regional Shore Operations Center ~ Combined Warfare Commander Operations
Navy Shore Operations Center (ShOC)

Establish integrated center and provide quality assurance of the Navy's shore operations; provide situational awareness and preliminary assessment to enable stakeholder effectiveness.
Integrated Model Operations Center, not just a dream…
NAVFAC – We are all Cyber Warriors
NAVFAC – Cyber Security RMF
Vendor Outreach

- Meeting with vendors to initiate information sharing
- Most now have test and development environments, IA Cyber
- Most are using Secure Software Development Lifecycle
- Exchanging inventory, known systems, integrators
- Exploring SME support for Fly-Away teams
- Moving from reactive to proactive, CYBERCOM and NSA support
- Providing eMASS and CSET hands on demos - suppliers, vendors, contractors, operations & maintenance staff are the eyes and ears, intrinsic part of the cyber solution
Cybersecuring DoD ICS Workshop

Cybersecuring DoD Industrial Control Systems
0800 – 0900 Overview of DoDI 8500/8510 RMF and PIT ICS, NIST Standards & Drivers, ICS Protocols
0900 – 0930 Overview of Shodan, Kali Linux, Samurai STFU, Wireshark
0930 – 1000 Using Shodan to Footprint ICS
1000 – 1015 Break
1015 – 1200 Using CSET 6.2: SAL, Network Arch Diagram, Inventory, Templates, Security Controls Evaluation, Reports, Data Aggregation & Trending, System Security Plan
1200 – 1300 Lunch
1300 – 1400 Using eMASS; hands on demonstration
1400 – 1430 Using the RMF KS ICS PIT website Step-By-Step instructions and Interim Excel files for uploading into eMASS
1430 – 1500 Wrap Up Q&A
Cybersecuring Building Control Systems

Introduction to Cybersecuring Building Control Systems
0800 – 0900 Classroom: Overview of Control Systems and Protocols
0900 – 1000 Classroom: Drivers, Standards, Guides, Publications
1000 – 1015 Break
1015 – 1115 Classroom: Defense in Depth, Enclaves, System Boundaries, Model Operations Center, Test and Development Environment, Continuous Monitoring
1115 – 1200 Lab: Using the DHS CSET and network mapping tools to create an Enclave, Network Diagram, and System Security Plan
1200 – 1300 Lunch
1400 – 1500 Lab: Introduction to Google Search & Hacking, Shodan, VMWare, Kali Linux, SamuraiSTFU tools
1500 – 1515 Break
1515 – 1600 Classroom: Attacking and Defending, Response and Recovery, Incident Reporting

Advanced Cybersecuring Building Control Systems
0800 – 0830 Hacker Methodology
0830 – 0900 Footprinting using Google Hacking, Google Earth, BING, Shodan, Kali Linux and SamuraiSTFU
0900 – 1000 Scanning and Enumeration using NMAP, WireShark, Sophia, SCAP and STIGS
1000 – 1015 Break
1015 – 1100 Advanced Meter Infrastructure Attack Methodology, AMI Penetration Testing
1100 – 1200 Using SamuraiSTFU ModbusPal Emulator, Packet Capture for Control System Analysis
1200 – 1300 Lunch
1300 – 1400 Exploitation using Metasploit, SamuraiSTFU
1400 – 1500 Privilege Escalation, Post Exploitation,
1500 – 1515 Break
1515 – 1600 Mitigation and Defense, Auditing, and Wrap Up

Army Mobile Weapons Platform

Truly air gapped….slight problem when firing in the forward position
Point is – maintain some level of manual operation, automation breaks!
Questions

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