Industrial Control Systems
Integration into the DoD Networks
A Briefing in Response to House Report 113-102, Accompanying the FY14 National Defense Authorization Act

Cyber Securing Control Systems

August, 2015
DoD Scope of Platform IT & Control Systems

- **Acquisitions / Weapon Systems**
  - H,M & E (ships / subs, missiles, UVs, etc.)
  - Training Simulators, 3D printing, etc.

- **EI&E**
  - Buildings & linear structures
  - Airfields, piers, life-safety, AT/FP & physical security, utility/environmental monitoring and control, other infrastructure

- **Medical**
  - Devices & equipment, pharmacy automation
  - Imaging, CAT, MRI, etc.

- **Logistics**
  - POLs, tank farms, pipelines, etc.
  - Warehousing, materials handling
  - Depots, refurbishment, plant mgmt.

- **Defense Industrial Base (DIB)**

*DoD IT & Cyber Strategies and Investments Progressing to Incorporate PIT / CS*
Installation Example:
CS Stakeholder Complexity
Tactical Power – Networked?

- Reduce Fuel Consumption
- Increase Portability
- Increase Sustainability
- Integrate Power with Platform
- Relevant Renewables
- Improve Soldier Power

Energy Efficiency Benefit AND or VS. Cybersecurity?
What’s in Your Building?

- “Smart” / High Performance Green Buildings
  - Since 2005 ~7,000+
  - Example: 5,000 desks, 15 floors, ~2M sqft
    o In-service / occupancy in 2011

- Fire Sprinkler System
- Interior Lighting Control
- Intrusion Detection
- Land Mobile Radios
- Renewable Energy Photo Voltaic Systems
- Shade Control System
- Smoke and Purge System
- Physical Access Control
- Vertical Transport System (Elevators and Escalators)

- Advanced Metering Infrastructure
  - Building Automation System
  - Building Management Control
  - CCTV Surveillance System
  - CO2 Monitoring
  - Digital Signage Systems
  - Electronic Security System
  - Emergency Management System
  - Energy Management System
  - Exterior Lighting Control Systems
  - Fire Alarm System

- 3 Networks Independently Managed

Unclassified - Distribution Statement A
Existing Integration Systems

Existing ICS Operating Software
US Chamber of Commerce – Dec 2011

CIO / IA Techs
• Not mine
• Not funded
• Not trained

Facility Mgr / Eng
• Not Mine
• Not funded
• Not trained

Which Group Best to Cyber Protect Control Systems?
Shodan Internet Connection Exploit

ICSA-12-228-01A: Tridium Niagara Vulnerabilities (Update A)
ICSA-15-029-01 : Honeywell HART DTM Vulnerability
ICSA-13-189-01 : QNX Multiple Vulnerabilities

Shodan – Tridium Search

HTTP/1.0 401 Unauthorized
WWW-Authenticate: Digest realm="Niagara-Admin", qop="auth", algorithm="MD5",
nonce="UvdraWNmNDAwNJE1ODc4NzBhYTc5NjMyYzIkJTlkYTk3NTg1ZDQy"
Content-Length: 56
Content-Type: text/html
Niagara-Platform: QNX
Niagara-Started: 2013-8-3-4-11-32   Baja-Station-Brand: distech
Niagara-HostId: Qnx-NPM2-0000-12EA-FDCC

Never Attribute Evil When Stupid is Still Available

Unclassified - Distribution Statement A
Cybersecurity Rules Apply to CS & Info Systems

- **DoDI 8500.01 Cybersecurity (14Mar14)**
  - Defines Platform Information Technology (PIT) [ICS]
  - Directs identify and centrally register at Component level
  - Directs use of NIST standards

- **DoDI 8510.01 Risk Management Framework (RMF) for DoD Information Technology (12Mar14)**
  - DIACAP replaced by RMF [goal: reduce C&A time 50%]
  - Manages life-cycle cybersecurity risk; promotes reciprocity

- Under SECDEF for Installations & Environment (OUSD(I&E) memo Real Property-related ICS Cybersecurity (19Mar14)

- NIST SP 800-82 r2 Guide to Industrial Control Systems (ICS) Security (May15)

- **DoDI 8530.01 Cybersecurity Activities Support to DoD Network Operations (FINAL DRAFT)**
  - DoD IN include systems operated by contractor, research centers, labs, agencies, non-DoD orgs
Based on DHS procurement document, DoD RMF, and GSA-DOD acquisition reform publications

Planning and Design
- Apply hardening criteria (e.g. DoD STIGS)
- Penetration Testing (artifacts)
- Complete initial CSET evaluation at 90% design, initial system security plan/baseline risk assessment
- Conform with relevant UFC and UFGS

Testing Use Cases:
SPIDERS, Fort Belvoir Microgrid

Construction
- 50-75% construction complete: conduct Factory Acceptance Testing (FAT) of major components
- 100% construction complete: conduct Site Acceptance Testing (SAT)
- Conduct Penetration Testing (e.g. SamuraiSTFU, special tool for ICS)
- Create System Security Plan (SSP)
- Create System Assessment Plan (SAP)
- Create CONOPS
- Create Plan of Action and Milestones (POAM)
- Create Incident Response Plan (IRP)
CSET 6.2 has new DoD, CNSS, NIST and DHS references & GM plugin

DoD Directed Standardized Assessments via CSET
DoD CIO RMF KS Portal – PIT/CS

EI&E Platform IT (PIT) Control Systems

Background

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

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

Key Documents and Tools

Overview of EI&E PIT Control Systems and Reference Architecture (pdf)

EI&E PIT Control Systems Glossary (pdf)

EI&E PIT Control System Master List (xlsx)

NIST SP 800-62 R2 Industrial Control Systems Security Guide (pdf)

NIST SP 800-62 R2 ICS Overlay Security Controls (agg)

NIST SP 800-62 R4 and NIST SP 800-52 R2 Version (Draft)

USACE Electronic Security Systems Performance Work Statement (1A Production) (pdf)

DHS Interagency Security Committee: Securing Government Assets through Combined Traditional Security and Information Technology (pdf)

DHS Cyber Security Evaluation Tool (CSET) (pdf)

GAO 15-3 Federal Facility Cybersecurity (pdf)

EI&E Control System and Information System Determination Process and Information Requirements for IT (pdf)

Figure 8 – Relationship of CSET, Component Registry, eMASS, and DIITPR

Build packages in CSET, export to eMASS or Component Registry

Component Registries

- APMS
- DADMS
- EITDR
- DHP SIRT

DIICAP

FUNDING

- MILCOM/ SRM
- Security
- Medical
- Logistics
- Weapons

RMF

- Authorization Package
- Control Overlay
- Inheritance
- Assess Only

eMASS

- System List
- Network Diagrams
- SSPs, POA&Ms
- Artifacts

Existing/Legacy Systems

Passive Monitoring Tools

Nessa, McAfee, Sophos, Grass Valley

Manage ATOs and IATTS

DoD Information Technology Portfolio Repository (DIITPR)

DoDITPR

Authorization Data Source for Portfolio Management

RMF KS PIT CS Website Released DoD-wide Aug’15

Unclassified - Distribution Statement A
DoD CIO Policy
RMF applies to all Information Technology

Reduces exploitation of vulnerabilities in PIT, Services, or Products previously not secured or assessed

“All DoD-owned or DoD-controlled IT that receive, process, display or transmit DoD information”

Not a One Size Fits All Approach to Securing IT

Unclassified - Distribution Statement A
Completed DIACAP Package Submitted to AO for Signature

<table>
<thead>
<tr>
<th>Completed DIACAP Package Submitted to AO for Signature</th>
<th>ATO Date</th>
<th>Maximum Duration of ATO under DIACAP</th>
</tr>
</thead>
<tbody>
<tr>
<td>DoD CIO Memo Date through May 31, 2015</td>
<td>Determined by AO Signature Date</td>
<td>2.5 years from AO signature date</td>
</tr>
<tr>
<td>June 1, 2015 through February 1, 2016</td>
<td>2 years from AO signature date</td>
<td></td>
</tr>
<tr>
<td>February 2, 2016 through October 1, 2016</td>
<td>1.5 years from AO signature date</td>
<td></td>
</tr>
</tbody>
</table>

Unclassified - Distribution Statement A
Joint Base Architecture for Secure Industrial Control Systems

- Detect, Mitigate, Recover
  - Develop TTP for defending DoD ICS / SCADA & PIT
  - Test topology based on networks found during surveys
  - Passive taps inserted for network monitoring
  - Test focused on SCADA network, CS network, and End Point Device network
  - Recognize enterprise network primarily used for attack positioning
  - 2nd “field test” completed July ‘15
  - TTP transition Dec ‘15

Monitor CS Networks For Malevolent / Unexpected Behavior
UFC Objectives

1. Define new Design and Construction Methodology to apply RMF & NIST SP 800-82 ICS Security Guide

2. Define IT / CS Reference Architecture as it applies to Control Systems

3. Verify controls @ 50-75% construction: conduct Factory Acceptance Testing (FAT) of major components

4. Verify controls @ 100% construction complete: conduct Site Acceptance Testing (SAT)

Pre-Final Version by 30 Sept ’15

Unclassified - Distribution Statement A
Cyber Range Control Systems?
An option: Camp Atterbury - Edinburgh, IN
• Critical infrastructure links to Industrial Control Systems-Supervisory Control and Data Acquisition (ICS/SCADA)
  a. Identify critical infrastructure dependent upon ICS/SCADA
  b. Validate Info Sys architecture supporting operation of ICS/SCADA
  c. Threat/Hazards identified to ICS/SCADA w/ appropriate countermeasures

• Have ICS / SCADA systems been identified that support infrastructure throughout the installation?

• Has a Risk & Threat Assessment on all ICS / SCADA systems been conducted IAW NIST SP 800-82, 800-30, and DoDI 8510.01?

• Are all appropriate ICS / SCADA Security Control Measures implemented IAW DoDI 8510.01 and NIST SP 800-53v4? [NIST SP 800-82 r2]
• DoD is transitioning to **smart buildings** increasingly utilizing wireless controls for heating, ventilation and air conditioning, security systems, lighting, electrical power, fire alarms, elevators, visitor controls, cellular communications, Wi-Fi networks, and first responder communications and other systems are increasing interconnected and online.

• Higher connectivity has increased the threat and vulnerability to cyber-attacks. Government Accountability Office study (GAO–15–6) highlighted the vulnerabilities and cyber risks to building and access control systems.

• Therefore, SECDEF to brief HASC **1/1/16** on the **cyber risks to smart buildings and access control systems** from **radio frequency systems** and **wireless communications**, and identification of **available technologies and practices available** to potentially **counter and mitigate** the identified security risks."
Challenge: Cyber security for control systems is a formidable effort; DoD requires insight to problem scope and solutions

Focus: 10 installations directly supporting operations [IE&OE]

3 Complementary Lines of Effort – 12 months
- DoD’s ICS Exposure to Internet Threats
- Gap Analysis of Tech. Solutions to Monitor DoD ICS
- Workforce Training Evaluation and Development

Benefits: Advances nascent ICS efforts in Defense community
- Give execs insight to set policy, reveal relevant cyber CS threats and vulnerabilities and gap between current and desired states
- Identify appropriate EI&E cyber workforce skills and requirements

JHU-APL Will Complete Assessments & Analysis w/ Service SMEs
Consistent Weak Link = WETWARE

DoD Cybersecurity Campaign memo (USCC, AT&L, CIO)

“Adversaries are actively attempting to access & establish a persistent presence in order to deny us access when most needed—and these threats continue to increase in scope and capability.”

“Most successful cyber attacks ...have been attributed to human error, either through improperly configured technological solutions or non-compliance with existing cybersecurity policy. Inspection reports continue to reveal Department-wide, systemic shortfalls in implementing basic cybersecurity requirements found in current policy, directives, and orders.”
Take-Away’s

• Include PIT/CS in ‘cyber-scape’ analysis

• Partner Facility Engineer & CIO SMEs

• Baseline: Establish Your PIT/CS “Position Zero”
  – Known inventory, topology, processes and tasks, users, data flows

• Implement routine monitoring to recognize deviations; determine legit / malicious

• Exercise methodology prior to needing it!

• Implement Alert process (register w/ DHS)

• **POC:** Mr. Daryl Haegley  daryl.r.haegley.civ@mail.mil