245 = Avg # Days Undiscovered Adversary

Manufacturing
• Logistics
• Transportation
• Facilities
• Medical
Same Commercial Device Installed Across DoD Enterprise
What’s in Your Building?
What’s on Your Installation?

- Public Works
  - Utility Mgmt
  - Renewable Energy
  - Facility Mgmt
- Emergency Services
  - EOC/IOC
  - Physical Security
- Installation Network Interface
- Water/Navigation Mgmt Systems
- Power
- Medical Systems
- Logistics / Transportation
- Environmental Control Systems
- Medical Device Network/Systems
- Fuel Cell Mgmt
- Lock/Dam Navigation Systems
- Water Quality/Level Reporting Systems
- Power Generation
- Fuel Transportation and Distribution
- WMD Transport Tracking systems
- Air Traffic Control
- Manufacturing/Maintenance/Safety Systems
- Rail Transport
- Railway/Railhead
- Ammo Supply Point

Other Agency Interfaces (Law Enforcement/DoD)
- LMR/First Responders
- CBRNE Sensors
- Fire Systems
- AT/FP Sensors
- Mobile Command
- Camera/Motion Sensors
- Intrusion Detection
- PACS
- Installation Entry Control
- Transport inspection systems
- Transport/warehousing RFID systems

Vendor/Contractor
- Remote Access/Data Sharing Web Interface
- Other Agency/Local PA

UNCLASSIFIED
COMMANDER, U.S. PACIFIC COMMAND
(USPACOM)
CAMP H.M. SMITH, HAWAII 96861-4028

February 11, 2016

The Honorable Ash Carter
Secretary of Defense
The Pentagon, Washington D.C.

Mr. Secretary,

We respectfully request your assistance in providing focus and visibility on an emerging threat that we believe will have serious consequences on our ability to execute assigned missions if not addressed – cybersecurity of DOD critical infrastructure Industrial Control Systems (ICS). We believe this issue is important enough to eventually include in your cyber scorecard. We must establish clear ownership policies at all levels of the Department, and invest in detection tools and processes to baseline normal network behavior from abnormal behavior. Once we’ve established this accountability, we should be able to track progress for establishing acceptable cybersecurity for our infrastructure ICS.

The Department of Homeland Security reported a seven-fold increase in cyber incidents between 2010 and 2015 on critical infrastructure (e.g., Platform Information Technology (PIT) systems, ICS, and Supervisory Control and Data Acquisition (SCADA) systems) that control the flow of electricity, water, fuel, etc. Many nefarious cyber payloads (e.g., Shamoon, Shodan, Havex and BlackEnergy) and emerging ones have the potential to debilitating our installations’ mission critical infrastructure.

As Geographic Combatant Commanders with homeland defense responsibilities and much at stake in this new cyber-connected world, we request your support.

Sincerely and Very Respectfully,

WILLIAM E. GORTNEY
Admiral, U.S. Navy
Commander, U.S. Northern Command

HARRY B. HARRIS
Admiral, U.S. Navy
Commander, U.S. Pacific Command

- Establish Clear Ownership
- Include in Scorecard
- Invest in Detection Tools
- 7x cyber incidents
“The threat is real and the risks are high, but our exposure is low…the control systems don’t connect to the internet.”

The risk of a damaging cyberattack is “greater than zero … the real threat is Mother Nature and humans doing stupid stuff.”

*Marcus Sachs, CSO of the North American Electric Reliability Corporation (NERC)*

**NERC SME: Utility Cyber Attack “Very Unlikely”**
What’s the Real Cyber Risk?

- Project SHINE (SHodan INtelligence Extraction) scanned the internet looking for SCADA and ICS devices. “Found more than 2 million (control) system devices directly connected to the Internet”
- Targeted ICS attacks in the US have caused, “loss of electric and water SCADA, damage to manufacturing lines, shutdown of HVAC systems, and damage to facility equipment including critical motors”

Control Systems Cybersecurity Expert, Joseph M. Weiss, recognized international authority on cybersecurity, control systems and system security

30yr SME: Utility Cyber Attack “Very Likely”
Many legitimate ICS files incorrectly flagged as malware in VirusTotal and other public sites

1,000s of legit ICS SW programs, HMI installers, data historian installers, & SW key generators

120 project files flagged as malicious and submitted to public databases, including a Nuclear Regulatory Commission report, substation layout specifics, maintenance reports, other types of sensitive information \{ inadvertently posted publicly \}

1,000s of cases of ICS software infected with viruses, just over the course of 90 days

3,000 unique industrial sites a year that are infected with traditional non-targeted malware

ICS Company: Utility Cyber Attack “Need Better Data”
What’s the Real Cyber Risk?

• Mar’16: RPA mission based in U.S. was flying a targeting mission overseas
• Routine maintenance power outage stateside, the RPA feed temporarily lost power
• Target was able to get "away and is able to continue plotting against the U.S. and our allies"

Was it Maintenance or Cyber? How Can You Tell?
<table>
<thead>
<tr>
<th>WHAT’S NEXT?</th>
<th>Target Retail Stores - 2013</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>….Your organization failed to consider impact of exploiting control systems….</strong></td>
<td>The attackers backed their way into network by compromising a 3rd-party vendor to steal data.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Kemuri Water Company - 2016</th>
<th>PLC ATTACK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hack accessed hundreds of PLCs used to manipulate control applications altering chemicals.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Ukraine Utilities - 2015</th>
<th>SCADA ATTACK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Left 225,000 customers in the dark. 1st successful cyber attack to knock a power grid offline.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Unnamed” Steel Mill, Germany - 2014</th>
<th>INSIDER ATTACK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hackers disrupted networks to access automation equipment resulted in massive damage.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>New York Dam - 2013</th>
<th>BACKDOOR ATTACK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Iranian hackers tried to open flood gates. Was this a dress rehearsal for something bigger?</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Saudi Aramco &amp; RasGas</th>
<th>ENTERPRISE ATTACK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Networks infected with the Shamoon virus erased information causing enterprise network outages.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>“Unnamed” Steel Mill - 2011</th>
<th>ENTERPRISE INFECTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Conficker worm infected the control network causing an instability in the communications.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Natanz Nuclear Facility - 2010</th>
<th>SCADA MALWARE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stuxnet infected the air-gapped control network bypassing causing damage to centrifuge.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Google HQ, Wharf - 2013</th>
<th>MISS-CONFIGURE</th>
</tr>
</thead>
<tbody>
<tr>
<td>SHODAN discovered over 21,000 miss-configured building automation systems.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Maroochy Water System - 2010</th>
<th>INSIDER ATTACK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disgruntled ex-employee hacks into the water system and floods the community of sewage.</td>
<td></td>
</tr>
</tbody>
</table>
Privatized Utility Services Overview

- DLA Contracted Utility Services
  - FY16 To Date: 4 contracts for 6 systems at 3 installations = $1.82B
  - FY15 Results: 3 contracts for 6 systems at 2 Installations = $339M
  - Results to Date: 76 contracts for 118 systems at 51 installations = $13.9B

- Cost Avoidance
  - Awarded contracts resulted in cost avoidance of $324M in FY16 / $2.6B overall

- Energy Security / Resiliency
  - Utilities Privatization program builds energy security/resiliency by improving utility systems. To date, System Owners have invested $412M in capital improvements

- On the Horizon
  - FY17: 12 contracts for 22 systems at 9 installations = $4.5B
  - Additional 43 systems in progress = $7.6B

Total Systems = 796

- 385 DoD systems have been privatized
- 548 DoD systems available to be evaluated

Awarded by Utility Services
Awarded by Others
In Process
FY 17 Projected Awards
Potential Future Workload

Privatized DoD Utilities - Who’s Cyber Accountable?
CIP
001 - Sabotage Rpt
002 - ID Crit Assets
003 - Min Sec Mgt
004 - Auth Access
005 - Elec Sec Param
006 - Impl PhySec
007 - Def M, P & P
008 - Rpt incidents
009 - Recovery Plans

Step
1 - Categorize
2 - Document
3 - Implement
4 - Assess
5 - Authorize
6 - Monitor
What’s the Risk of Exposing Energy Consumption Data?

Facility Level

- Generators for individual critical loads

Site / Campus Level

Usage or Criticality?

Regional / Enterprise Level

“All Energy Data is UNCLASSIFIED”…True?
Cybersecurity Controls Apply to New Construction

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)
Advanced Cybersecurity for Industrial Control Systems Tactics Techniques Procedures (ACI TTPs) was an OSD funded, Army Test and Evaluation managed, Joint Test to develop defensive cyber TTPs to detect, mitigate, and recover ICS / SCADA from nation-state level of cyber attacks.

Network managers supporting DoD ICS lack TTP to detect, mitigate, and recover from nation-state level cyber attacks.

Updated Jan’17
DoD IG Audit

• “Determine whether DoD is implementing cybersecurity controls to protect, detect, counter and mitigate potential cyber attacks on control systems supporting DoD critical missions / assets.”

• Visit 5 AF Sites: Aug-Nov’16
• Discussion draft: Dec’16
• Draft report: Feb’17
• Final report: Apr’17
Mission Assurance Assessment Benchmarks (MAA)

- Is the cybersecurity office aware of ICS in use on the installation?
- Does the system control critical or mission related utilities?
- Does the ICS have connectivity to installation data or telecom networks?
- Have the ICS systems gone through the Security Authorization process (Security Risk Management Framework)?
- Has risk assessment been completed?
- Does the ICS organization use Role-Based Access Control to restrict ICS user privileges to only those that are required to perform their job responsibilities (i.e., configuring each role based on the principle of least privilege)?
- Are data flow controls tested to ensure that other systems cannot directly access devices within the ICS environment?
- Are firewalls implemented to enforce security policies?
- Does the ICS organization implement a security plan that concentrates on continuous security improvements and focuses on the life cycle of the system?
- Does the ICS organization implement an effective defense-in-depth strategy?
EVALUATION OF CYBER VULNERABILITIES OF DOD CRITICAL INFRASTRUCTURE

- Submit plan w/in 180 days (Jun’17 / Sep’17)
- Select 2 installations
- Assess critical infrastructure via DoD/DoE lab “pilot”
- Provide results by Dec 2019
- Develop strategies mitigating risks of cyber vulnerabilities by Dec 2020
- $0

JS, Services, OSD, Labs Collaboration
Embracing Silicon Valley Crowdsourcing: “Bug Bountys” Will Utilities & ICS be Next?

Hacking the Pentagon

Cost: $175K vs. Typical Contractor $1M
What’s in Your Cloud?

- **Infrastructure as a Service (IaaS)**
  - provide pay-per-utility pricing, dynamic scaling, security control, faster provisioning and guaranteed performance levels

- **Platform as a Service (PaaS)**
  - deliver lower operational cost, faster development, and seamless integration

- **Software as a Service (SaaS)**
  - improves upgrade cycle times, automated backups, and location independence

**Better to Outsource Like UP?**
Links to FREE DoD & Commercial Resources

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

http://www.wbdg.org/resources/cybersecurity.php

“Cyber Trust” Rating...What’s Yours?

- Rating # Correlates to Breach Potential
- Detailed Event and Configuration Information via External Parties
Analysis of 27,458 companies reveals companies with ratings >400 are 5X more likely to have experienced a publicly disclosed breach.
Discussion

Information Systems

Control Systems

Who’s Role? Detect, Mitigate & Recover from Cyber Exploit
DoD & Commercial Resources

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

Department of Defense Advanced Control System Tactics, Techniques, and Procedures (TTPs) 2017:

UFC 4-010-06 CYBERSECURITY OF FACILITY-RELATED CONTROL SYSTEMS Sept 2016
https://wbdg.org/ffc/dod/unified-facilities-criteria-ufc/ufc-4-010-06

Strategic Environmental Research and Development Program (SERDP) and Environmental Security Technology Certification Program (ESTCP) [info & funding solicitations]

DoD OASD(EI&E) and Federal Facilities Council (FFC), under the National Research Council (NRC) sponsored a 3-day Building Control System Cyber Resilience Forum in Nov ‘15.
http://sites.nationalacademies.org/DEPS/FFC/DEPS_166792

DoDI 5000.02 Cybersecurity in the Defense Acquisition System Jan 2017

Whole Building Design Guide website cyber references
http://www.wbdg.org/resources/cybersecurity

Tools
https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-176-02A
https://ics-cert.us-cert.gov/tips/ICS-TIP-12-146-01B

Workshops / Building Control Systems Cyber Security Training

Industrial Control Systems Joint Working Group (ICSJWG)_