

- Manufacturing
- Logistics
- Transportation
- Facilities
- Medical

Source: GAO. | GAO-15-8

245 = Avg # Days Undiscovered Adversary
DHS ICS CERT

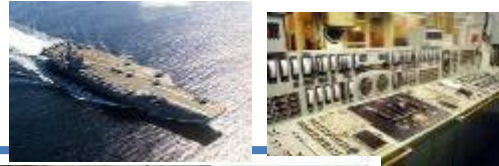
UNCLASSIFIED

Operational Energy

Weapon Platforms

Buildings

>500 Installations
>250K Buildings
>200K Structures



Electrical and HVAC



Pumps and Motors



Nuclear



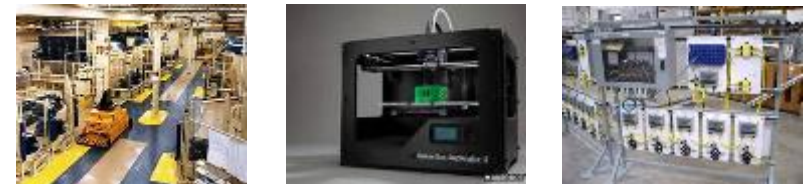
Vehicles/Charging



Typical Controller

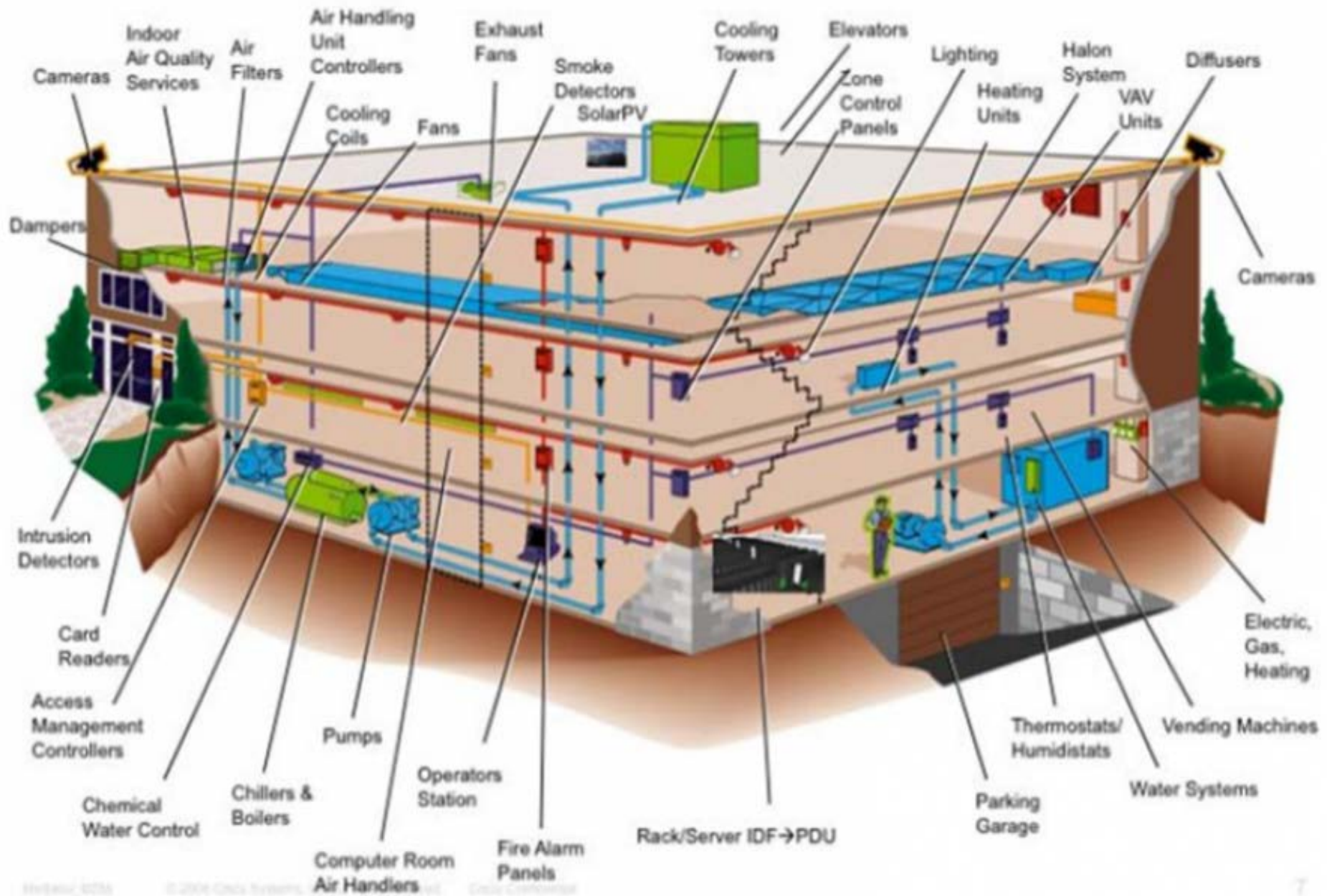
Medical

Manufacturing

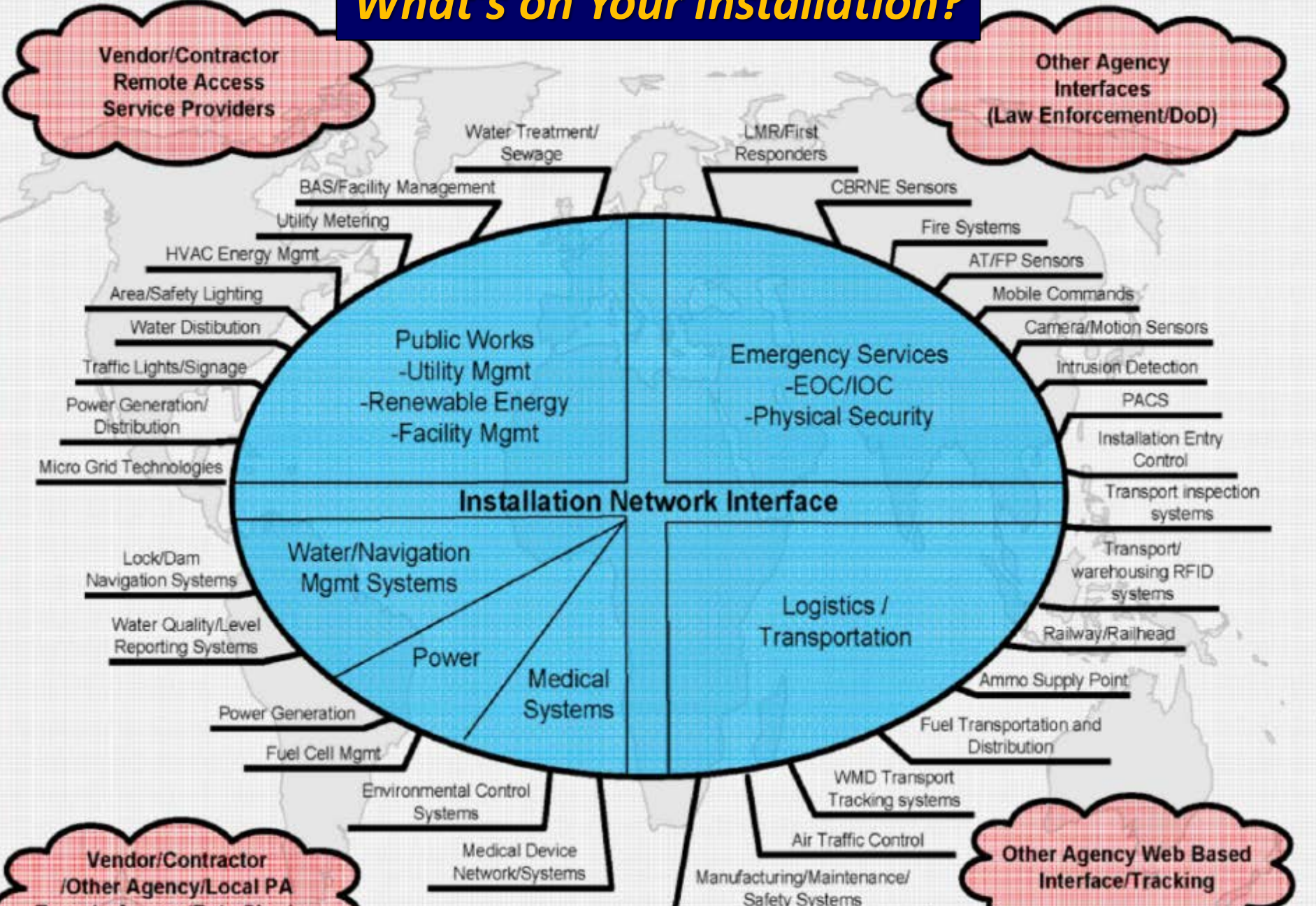


Same Commercial Device Installed Across DoD Enterprise

What's in Your Building?



What's on Your Installation?



UNCLASSIFIED

“8 Star Memo”

Cybersecurity of DoD Critical Infrastructure ICS



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 debilitate 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

Sincerely and Very Respectfully,

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



What's the Real Cyber Risk?

“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”

(Malware in Modern ICS)

- 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?

WHAT'S NEXT?

....Your organization failed to consider impact of exploiting control systems....

Target Retail Stores - 2013

BACKDOOR ATTACK



The attackers backed their way into network by compromising a 3rd-party vendor to steal data.

Kemuri Water Company - 2016

PLC ATTACK



Hack accessed hundreds of PLCs used to manipulate control applications altering chemicals.

Saudi Aramco & RasGas

ENTERPRISE ATTACK



Networks infected with the Shamoon virus erased information causing enterprise network outages.

Ukraine Utilities - 2015

SCADA ATTACK



Left 225,000 customers in the dark. 1st successful cyber attack to knock a power grid offline.

Project Basecamp - 2012

PLC ATTACK



A team used a penetration test on PLCs to realize how badly vulnerable their SCADA/ICS were .

“Unnamed” Steel Mill, Germany - 2014

INSIDER ATTACK



Hackers disrupted networks to access automation equipment resulted in massive damage.

“Unnamed” Steel Mill - 2011

ENTERPRISE INFECTION



The Conficker worm infected the control network causing an instability in the communications.

New York Dam - 2013

BACKDOOR ATTACK



Iranian hackers tried to open flood gates. Was this a dress rehearsal for something bigger?

Natanz Nuclear Facility - 2010

SCADA MALWARE



Stuxnet infected the air-gapped control network bypassing causing damage to centrifuge.

Google HQ, Wharf - 2013

MISS-CONFIGURE



SHODAN discovered over 21,000 miss-configured building automation systems.

Maroochy Water System - 2010

INSIDER ATTACK



Disgruntled ex-employee hacks into the water system and floods the community of sewage.

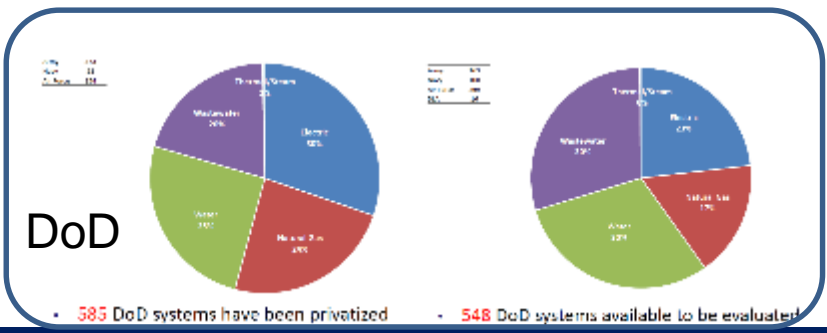


UNCLASSIFIED

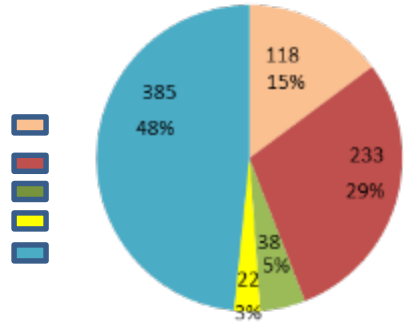
Privatized Utility Services Overview

- 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



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



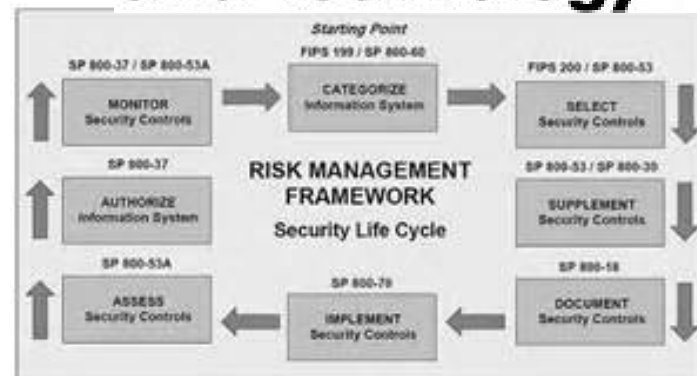


NIST

National Institute of Standards and Technology



Federal Energy Regulatory Commission



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

DHS ICS-CERT / CSET 8.0

September 15 October 2016



ICS-CERT Overview

ICS-CERT Vulnerability Coordination

Is a state of the industry to highlight ICS-CERT Vulnerability Coordination


The primary objective of the Industrial Control System Cyber Emergency Response Team (ICS-CERT) Vulnerability Coordination Team is to identify and coordinate the response to vulnerabilities in ICS systems. The team will coordinate with the ICS community to identify and coordinate the response to vulnerabilities in ICS systems. The team will coordinate with the ICS community to identify and coordinate the response to vulnerabilities in ICS systems.

Reliability Coordination Process

1. Detection and Collection
2. Analysis
3. Mitigation Coordination
4. Application of Mitigation
5. Disclosure

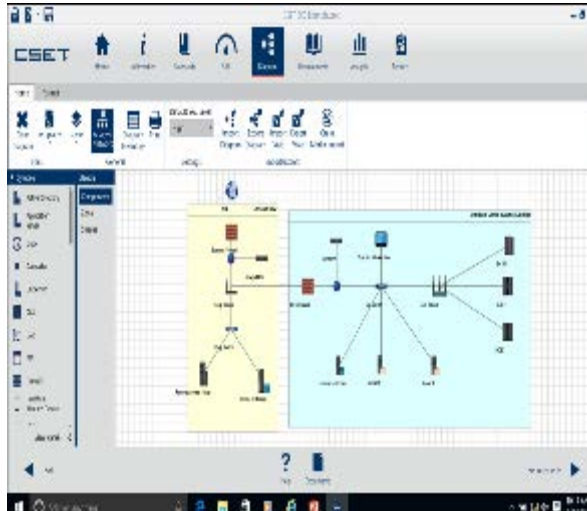

33-CERT
This is a publication of the Industrial Control System Cyber Emergency Response Team (ICS-CERT) for the purpose of the Department of Homeland Security (DHS) National Cybersecurity and Communications Incident Response Center (NCCIRC). ICS-CERT was created to coordinate the response to vulnerabilities in ICS systems. The team will coordinate with the ICS community to identify and coordinate the response to vulnerabilities in ICS systems.

Contact Information
33-CERT is the point of contact for ICS-CERT. For more information, contact 33-CERT at 1-877-751-7311. Visit the ICS-CERT website at www.ics-cert.gov.

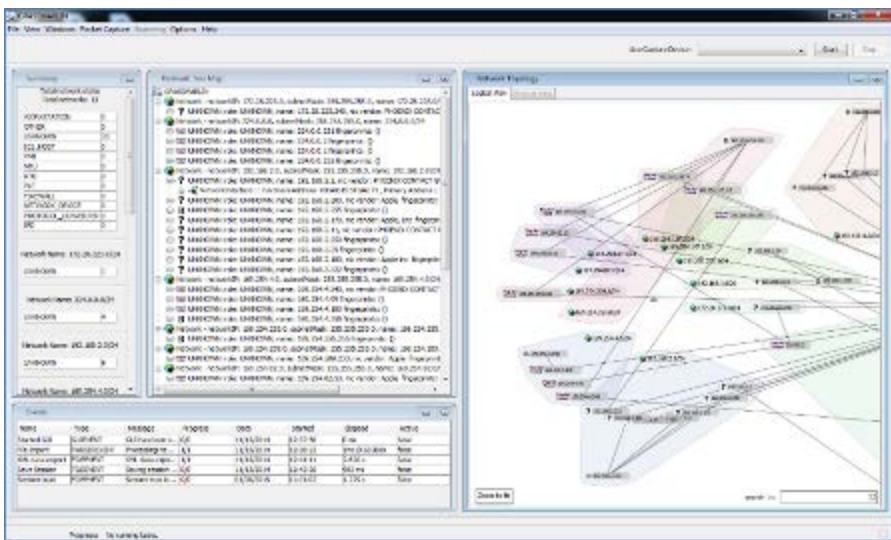


Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies

Industrial Control Systems Cyber Emergency Response Team
September 2016

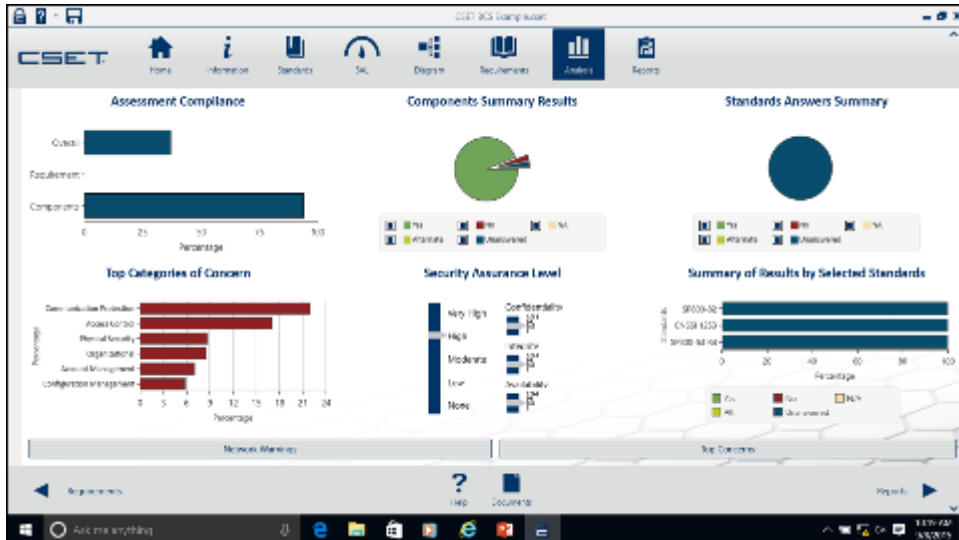


CSET Dashboard Overview: Shows network topology, assessment compliance, and components summary results.



Network Topology View: Displays a detailed network diagram with nodes and connections. Includes a list of nodes on the left and a table at the bottom.

Name	IP	MAC	Vendor	OS	OSVer	OSBuild	HWVer
10.10.10.1	10.10.10.1	0800:0000:0000:0000	HP	Windows	6.0.6002	6002.8171.amd64	None
10.10.10.2	10.10.10.2	0800:0000:0000:0000	HP	Windows	6.0.6002	6002.8171.amd64	None



Assessment Compliance: Shows a bar chart with 'Compliance' at approximately 85%.

Category	Percentage
Default Admin Privilege	~22%
Default Admin	~18%
Default Admin Access	~15%
Default Admin Control	~12%
Default Admin Management	~10%
Default Admin Configuration	~8%

Security Assurance Level: Shows a vertical scale from None to Very High.

Summary of Results by Selected Standards: Shows a bar chart for standards like SP800-82, CS-101, etc.

What's the Risk of Exposing Energy Consumption Data?

Facility Level



- Generators for individual critical loads




Usage or Criticality?

Site / Campus Level

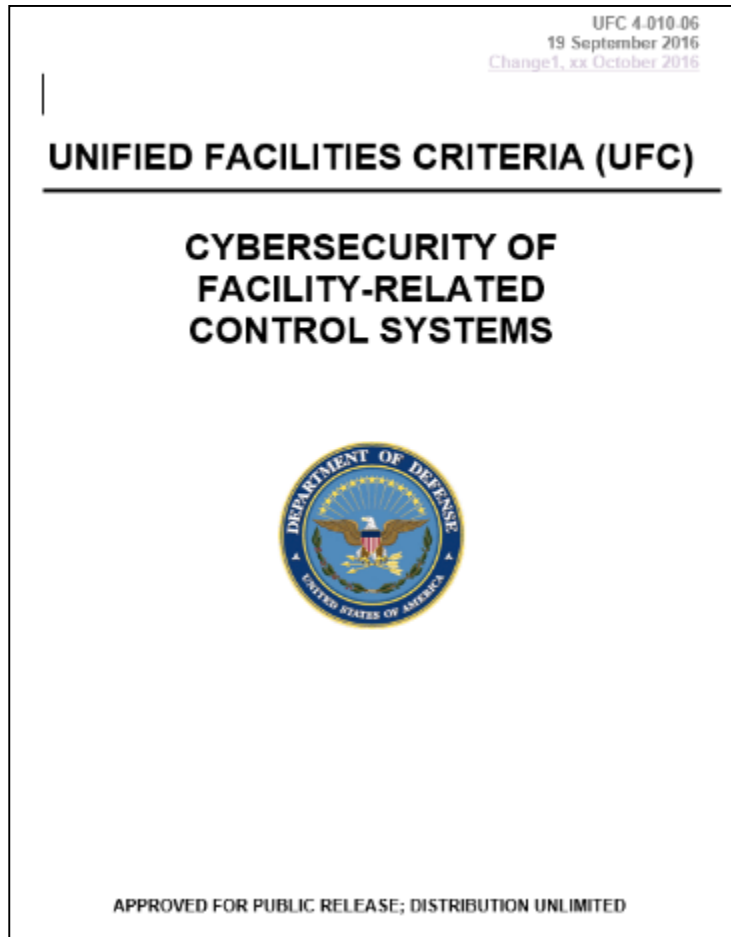


Regional / Enterprise Level



"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)

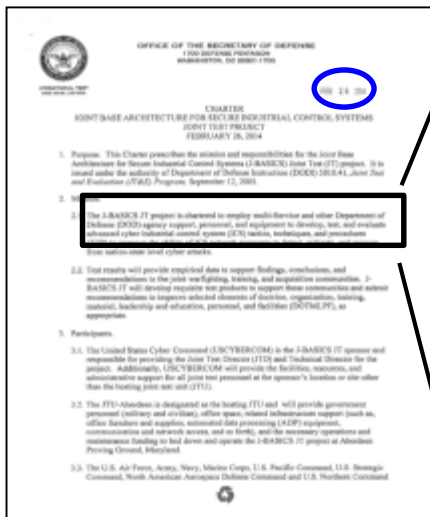
UFC 4-010-06 Published 19 Sept '16

ACI TTP

Charter

FEB 26 2014

“employ multi-Service and other Department of Defense (DoD) agency support, personnel and equipment to develop, test, and evaluate advanced cyber industrial control system (ICS) tactics, techniques, and procedures (TTP) to improve the ability of ICS network managers to detect, mitigate, and recover from nation-state level cyber attacks”



Lead Sponsor

USCYBERCOM

Operational Endorsers

NORAD-NORTHCOM

OASD (AT&L) / EI&E

USPACOM

USSTRATCOM



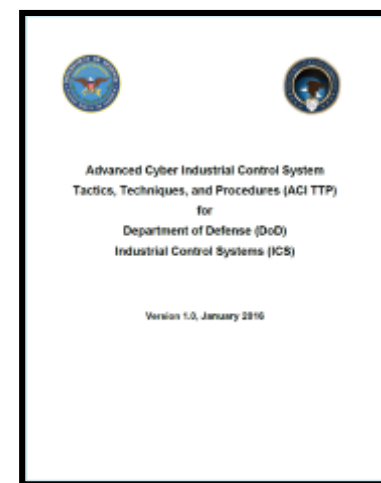
Background

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.

Updated Jan'17

Problem Statement

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





INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22304-1500

May 3, 2016

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR ACQUISITION,
TECHNOLOGY, AND LOGISTICS
ASSISTANT SECRETARY OF THE AIR FORCE
(FINANCIAL MANAGEMENT AND COMPTROLLER)
DOD CHIEF INFORMATION OFFICER
NAVAL INSPECTOR GENERAL
AUDITOR GENERAL, DEPARTMENT OF THE ARMY

SUBJECT: Audit of Control Systems Cybersecurity (Project No. D2016-D000RB-0149.000)

We plan to begin the subject audit in May 2016. This is the first in a series of audits on the security of control systems that support DoD critical missions or assets. Our objective is to determine whether DoD has implemented cybersecurity controls to protect, detect, counter, and mitigate potential cyberattacks on control systems supporting DoD critical missions or assets. We will consider suggestions from management on additional or revised objectives.

We will perform the audit at the Offices of the Under Secretary of Defense for Acquisition, Technology, and Logistics, the DoD Chief Information Officer, and selected Military Service activities. We may identify additional locations during the audit.

Please provide us with a point of contact for the audit within **10 days** of the date of this memorandum. The point of contact should be a Government employee—a GS-15, pay band equivalent, or the military equivalent. Send the contact's name, title, grade/pay band, phone number, and e-mail address to audrco@dodig.mil.

You can obtain information about the Department of Defense Office of Inspector General from DoD Directive 5106.01, "Inspector General of the Department of Defense (IG DoD)," April 20, 2012; DoD Instruction 7600.02, "Audit Policies," October 16, 2014; and DoD Instruction 7050.03, "Office of the Inspector General of the Department of Defense Access to Records and Information," March 22, 2013. Our website is www.dodig.mil.

If you have any questions, please contact Mr. Robert F. Prinzbach II at (703) 604-8907, (DSN 664-8907)/Robert.Prinzbach@dodig.mil, or Mr. Matthew Pitzer at (703) 604-9173, (DSN 664-9173)/Matthew.Pitzer@dodig.mil.

Carol N. Gorman
Assistant Inspector General
Readiness and Cyber Operations

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?



NDAA 17 SEC. 1650

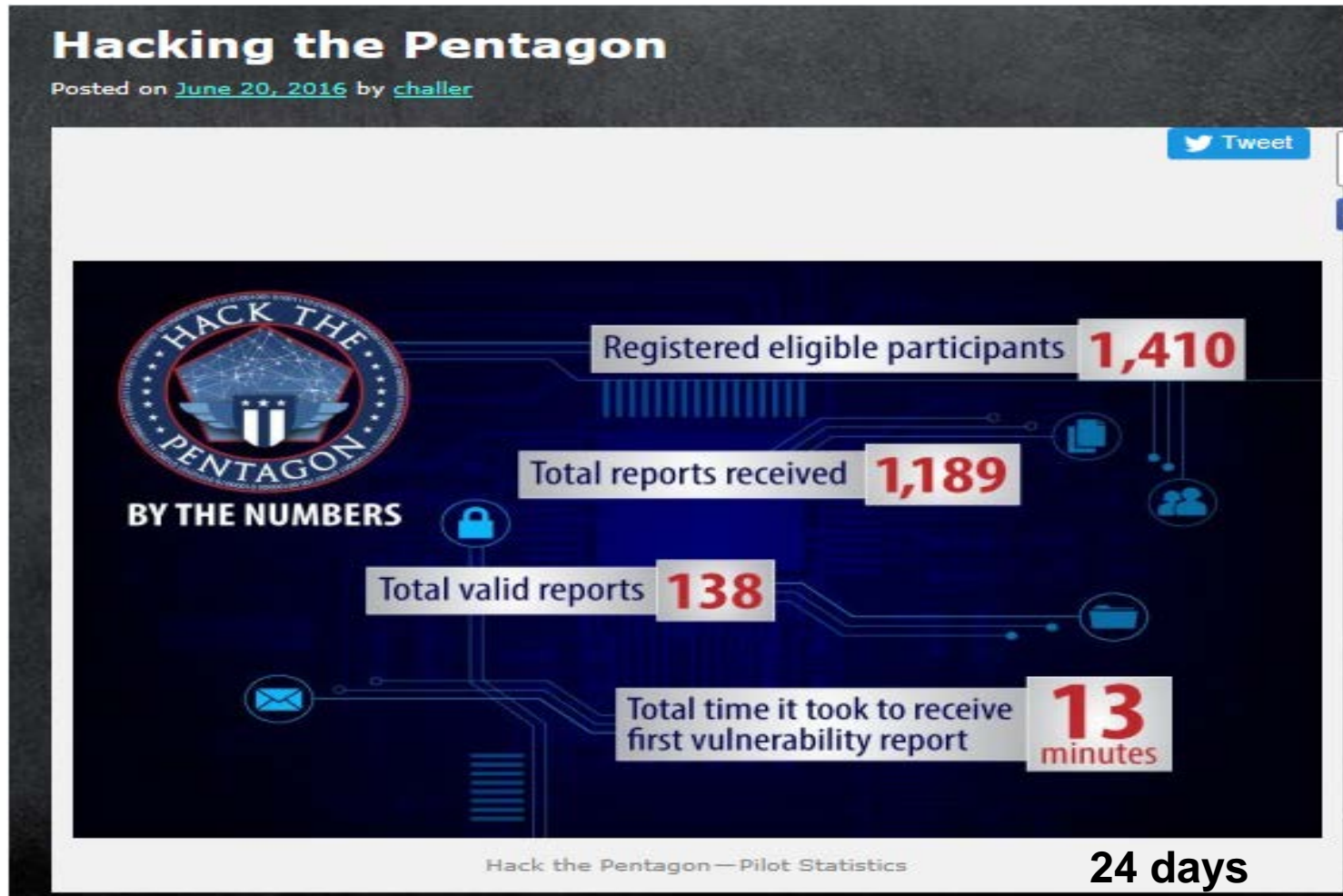


EVALUATION OF CYBER VULNERABILITIES OF DOD CRITICAL INFRASTRUCTURE

- 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

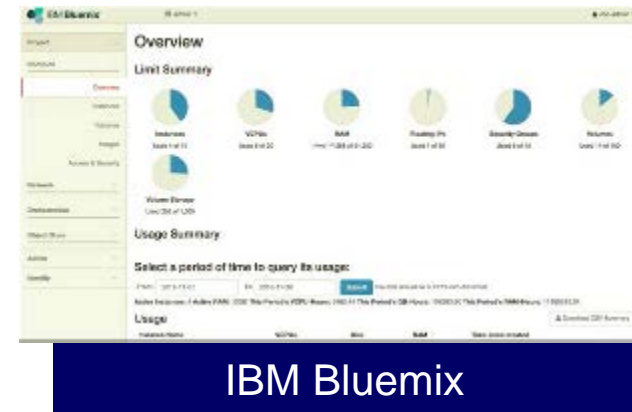
Embracing Silicon Valley Crowdsourcing: “Bug Bountys” *Will Utilities & ICS be Next?*



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?

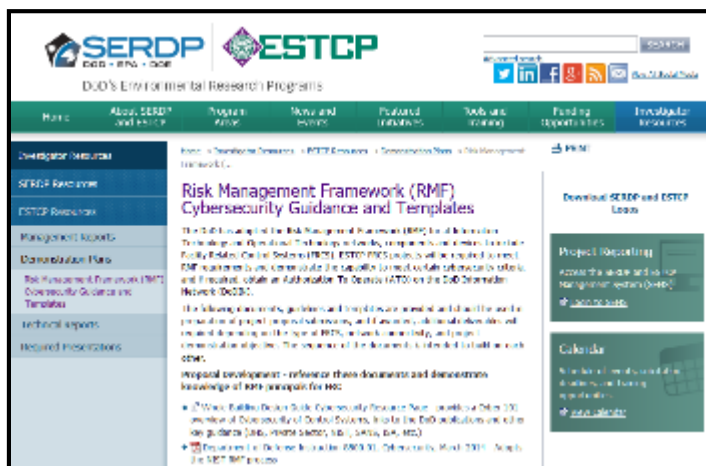
Links to FREE DoD & Commercial Resources



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



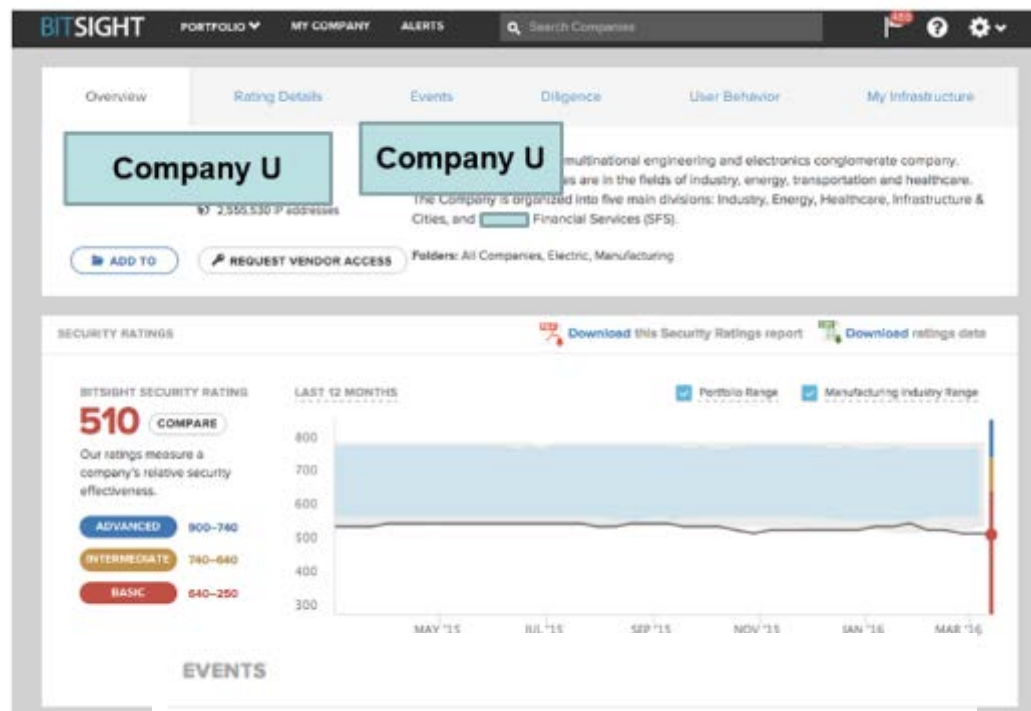
<http://www.wbdg.org/resources/cybersecurity.php>



<https://serdp-estcp.org/Investigator-Resources/ESTCP-Resources/Demonstration-Plans/Risk-Management-Framework-RMF-Cybersecurity-Guidance-and-Templates>

“Cyber Trust” Rating...What’s Yours?

- Rating # Correlates to Breach Potential
- Detailed Event and Configuration Information via External Parties



EVENTS

Botnet Infections	F
Spam Propagation	B
Malware Servers	A
Unsolicited Communication	B
Potentially Exploited	C

DILIGENCE

SPF Domains	C
DKIM Records	F
TLS/SSL Certificates	C
TLS/SSL Configurations	B
Open Ports	C
DNSSEC Records ^{beta}	C
Application Security ^{beta}	C

USER BEHAVIOR

File Sharing	D
--------------	---

OTHER

Data Breaches	A
---------------	---

Events are observed incidents of compromise on a company's network. These include risk vectors such as botnet infections and malware servers. Industry averages are calculated from similarly sized companies.

THIS WEEK PAST YEAR AVERAGE EVENT DURATION

10 **1,416** **2.8 days**

3.4% faster to resolve events than the Manufacturing industry average.

2.8 days **Company U**

2.1 days Portfolio average

2.9 days Manufacturing industry average

SECURITY RATING LEGEND:

ADVANCED (900-740)

INTERMEDIATE (740-640)

BASIC (640-250)

Company	Trend	Rating
[Redacted]		580
[Redacted]		630
[Redacted]		720
[Redacted]		710
[Redacted]		770
[Redacted]		710
[Redacted]		680
[Redacted]		600
[Redacted]		650
[Redacted]		380

Company	Trend	Rating
[Redacted]		750
[Redacted]		760
[Redacted]		750
[Redacted]		660
[Redacted]		590
[Redacted]		750
[Redacted]		730
[Redacted]		490
[Redacted]		560

ABOUT BITSIGHT

BitSight Technologies' mission is to provide organizations with the insight they need to proactively identify, quantify and mitigate

security risk. The company's platform continuously collects and analyzes vast amounts of external evidence on security behaviors in order to help organizations make timely, data driven risk management decisions. Based in Cambridge, MA, BitSight Technologies was founded in 2011. For more information, please visit www.bitsighttech.com or follow BitSight on Twitter @BitSight.

BITSIGHT

Security Rating Report

PORTFOLIO STATISTICS

COMPANIES

19

IP ADDRESSES

9,868,600

INDUSTRIES

5

MEDIAN SECURITY RATING

660

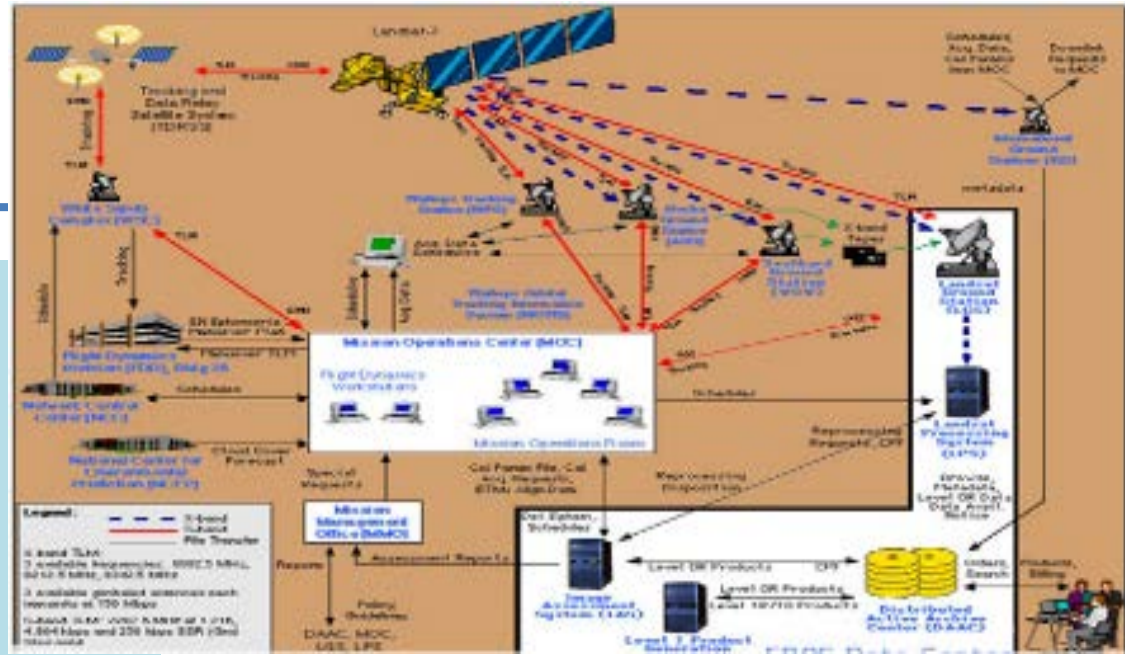
RANGE OF SECURITY RATINGS

380-770

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:
http://www.wbdg.org/pdfs/aci_ttp_rev1_2017.pdf

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]
<https://serdp-estcp.org/Investigator-Resources/ESTCP-Resources/Demonstration-Plans/Cybersecurity-Guidelines>

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
http://www.dtic.mil/whs/directives/corres/pdf/500002_dodi_2015.pdf

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
<http://hpac.com/training/workshop-what-do-when-building-control-systems-get-hacked-set>

Industrial Control Systems Joint Working Group (ICSJWG_
<https://ics-cert.us-cert.gov/Industrial-Control-Systems-Joint-Working-Group-ICSJWG>