The PMC Group LLC

Engineering a better tomorrow today

Cybersecurity of Buildings Workshop – *OT and IT Convergence – A New Paradigm*

January 28, 2014

National Institute of BUILDING SCIENCES

An Authoritative Source of Innovative Solutions for the Built Environment

Agenda

9:00 – 9:10	Welcome and Introductions: Henry Green
9:10 – 9:15	Opening Remarks: Sue Armstrong
9:15 – 10:00	Overview of Major Building Cyber Programs and Initiatives: Michael Chipley and Earle Kennett
10:00 – 10:30	DHS ISC Converged Systems Overview: Will Morrison or Bernard Holt
10:30 – 10:45	**Break**
10:45 – 11:15	DHS NCCIC, ICS-CERT and CSET: Tool Lisa Kaiser
11:15 – 11:45	Industry Viewpoint: Tim Owens, Tim Alexander
11:45 – 1:00	**Lunch**
1:00 – 1:30	DHS ISC Converged Technologies implementation in the agency: Matt Weese and Chris Coleman
1:30 – 2:00	Workgroup Topics: Model Ops Center, Model Test and Development Environment, Penetration Testing
2:00 – 2:30	Workgroup Topics: Information Sharing, Automated Vulnerability and Patch Management, White Listing
2:30 – 3:00	Workgroup Open Discussion, Next Steps, Adjourn

The PMC Group LLC

Engineering a better tomorrow today

Overview of Building Control Systems Cybersecurity Efforts

Michael Chipley, PhD PMP LEED AP
President

January 28, 2014

mchipley@pmcgroup.biz

Draft DHS ISC White Paper

Most often, security professionals procure and employ IT assets and infrastructure to obtain protection in depth for tangible and intangible assets for which the security organization is responsible. The layered security approach may include Closed-Circuit Video Equipment (CCVE) or video systems, intrusion detection systems (IDS) and electronic physical access control systems (PACS) either as stand-alone or an integrated environment to accomplish the tasks of deterrence, detection, delay, and response, and to serve as a force multiplier for security staff assigned to achieve those and other tasks.

To facilitate an understanding of the necessary interaction between traditional security and information technology (IT) communities, the Interagency Security Committee (ISC) developed the recommendations contained herein to provide traditional security and IT professionals with mechanisms to support security programs while integrating information assurance management controls.

Draft DHS ISC White Paper

Federal agencies must meet the minimum security requirements through the use of the security controls in NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems [NIST SP 800-53]. NIST SP 800-53 contains the management, operational, and technical safeguards or countermeasures prescribed for an information system, enabling agencies to assess security controls considering the Risk Management Framework (RMF). The assessment identifies security controls in place, providing a determination on the level and quality of employed risk management framework, and provides information on strengths and vulnerabilities on physical security IT systems.

Draft DHS ISC White Paper

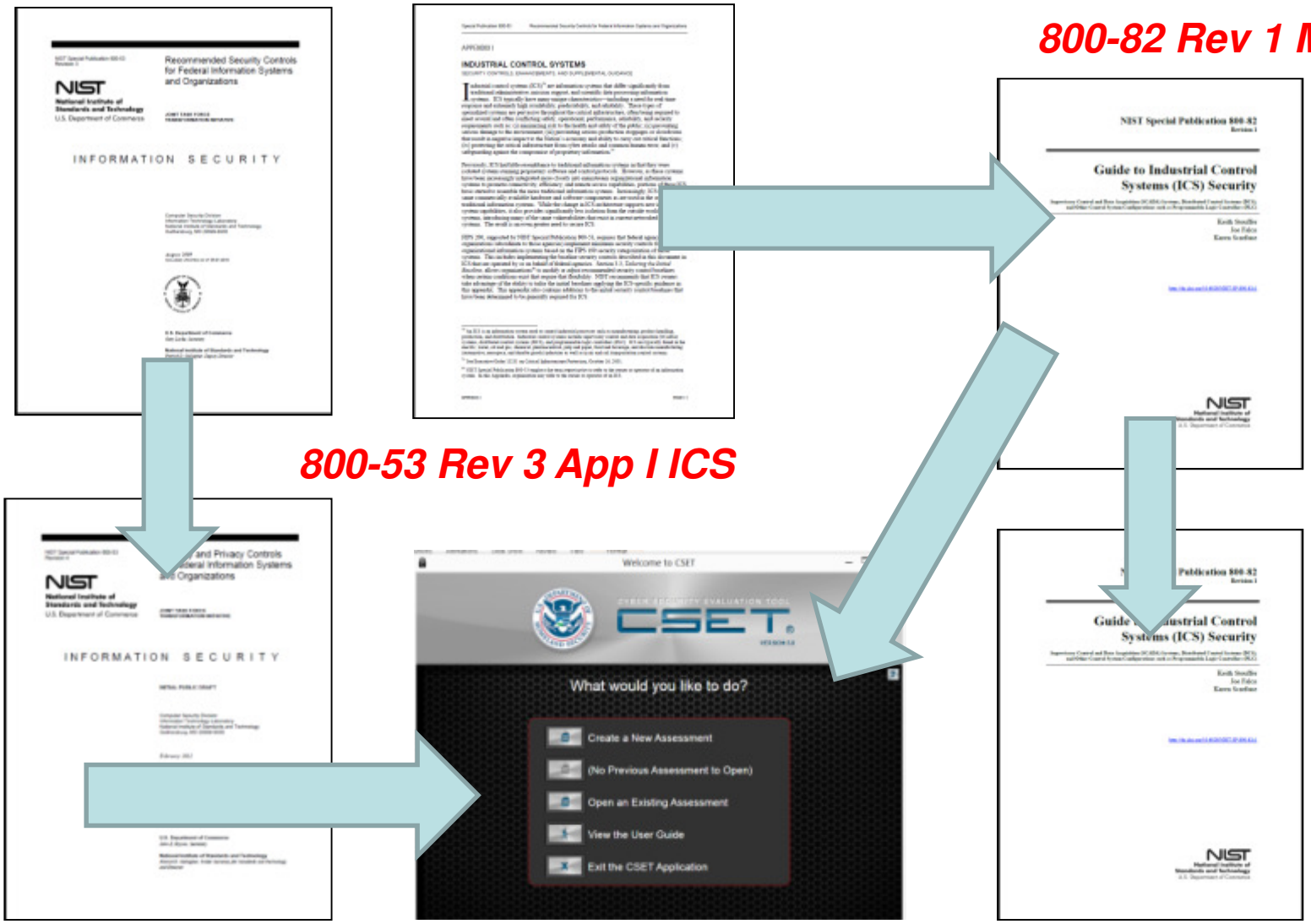
1 **Table 1: Core Team Members and Descriptions**

CORE TEAM	
Team Member	**Role/Responsibility**
Chief Security Officer (CSO), or designee	Provide and ensure compliance with all national and agency specific guidelines to include but not limited to credentialing, facility access, logical access, and security systems.
Chief Information Officer (CIO), or designee	Vet and or approve hardware/software implementation and or integration onto agency network by following agency specific policy or guidance.
Security Specialist	Ensure FSA is complete, ISC recommendations are accurate, national and agency policies and directives are incorporated, and compliance with agency specific requirements.
Internet Technology (IT) Specialist	Validate agencies switch and IP port selections for logical/physical access and or security components utilizing the agencies network as well as ensuring security of agencies network systems by working in conjunction with contractors on-site.
Facility Manager	Ensuring adherence with all municipal and state regulations in regards to systems implementation (e.g., fire safety codes).
Facility Engineer	Provide expertise on facility infrastructure including but not limited to primary electrical and phone trunks, power grids/sources, demarcation locations and acts as the conduit with utility providers.
Property Owner/Lessor	Provides guidance and approval of equipment installation on/or within facility, acts as liaison with municipal and state inspectors.
Security Integrator/Contractor	Performs physical installation of security components as well as provides guidance on security implementation, future/end state, and national directives.

2

DRAFT

NIST SP 800-53 and SP 800-82



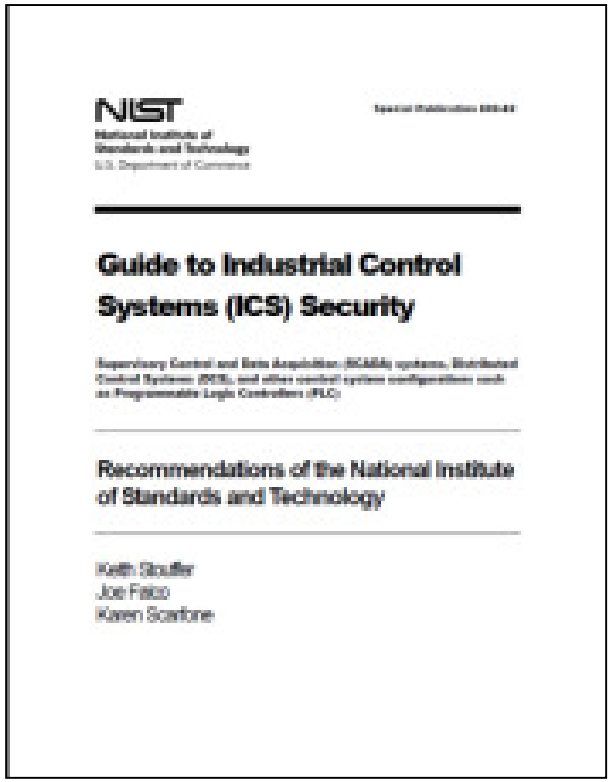
Industrial Control Systems (ICS)

Industrial Control Systems (ICS) are physical equipment oriented technologies and systems that deal with the actual running of plants and equipment, include devices that ensure physical system integrity and meet technical constraints, and are event-driven and frequently real-time software applications or devices with embedded software. These types of specialized systems are pervasive throughout the infrastructure and are required to meet numerous and often conflicting safety, performance, security, reliability, and operational requirements. ICSs range from Building Automation Systems (BAS), Building Management Systems (BMS), Energy Management Systems (EMS), Emergency Management Information Systems (EMIS), and Electronic Security Systems (ESS).

Within the controls systems industry, ICS systems are often referred to as Operational Technology (OT) systems.

Emerging Terms: Cyber-Physical Systems (CPS), Resilient Interdependent Infrastructure Processes and Systems (RIPS)

Standards - NIST 800-82 Rev 1 and 2


NIST

Guide to Industrial Control Systems (ICS) Security

Recommendations of the National Institute of Standards and Technology

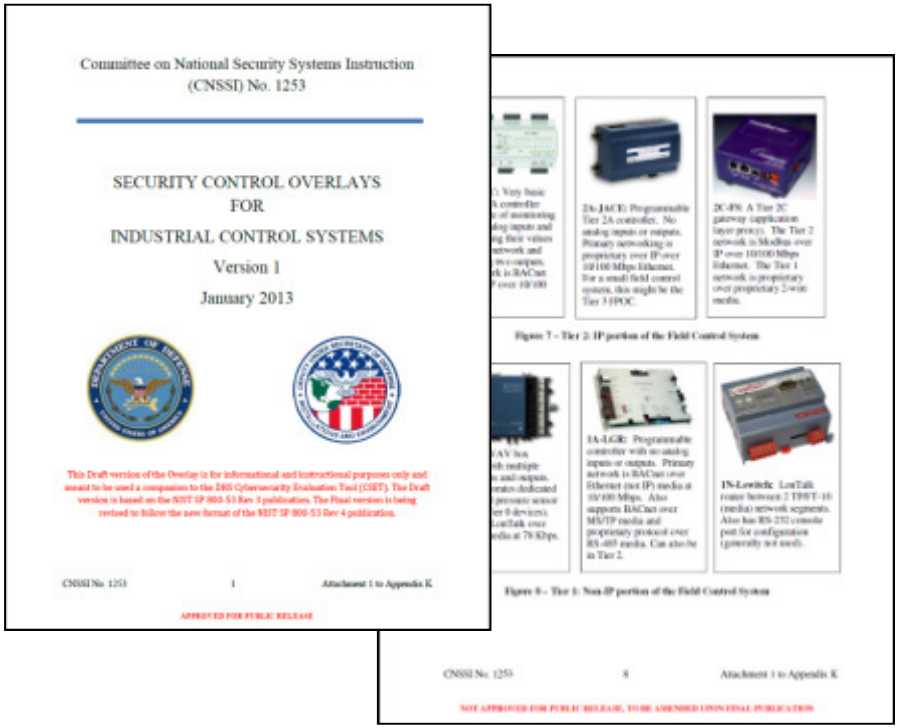
Keith Stouffer
Joe Falco
Karen Scarfone

This document provides guidance for establishing secure industrial control systems (ICS). These ICS, which include supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as skid-mounted Programmable Logic Controllers (PLC) are often found in the industrial control sectors.

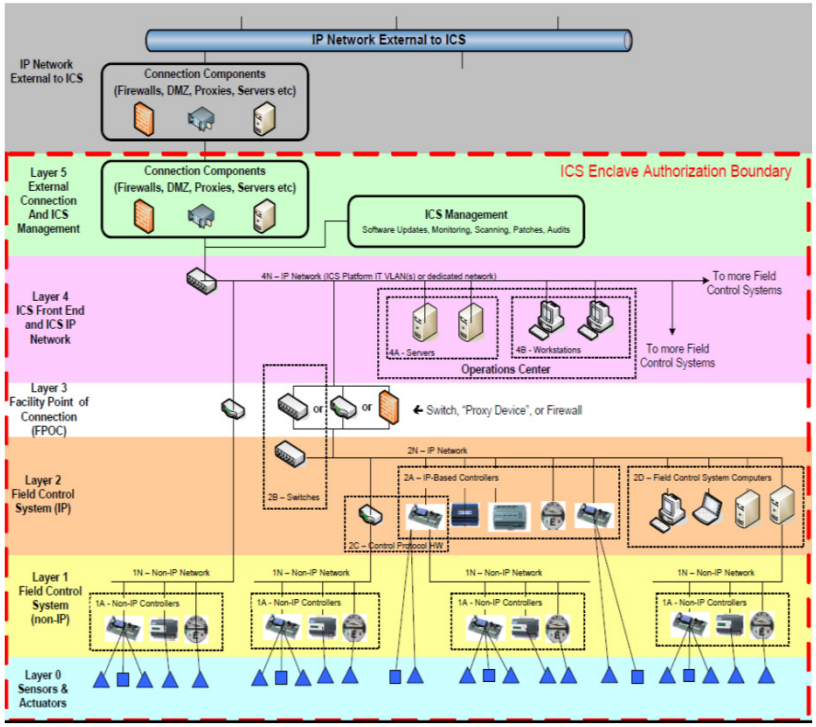
This document provides an overview of these ICS and typical system topologies, identifies typical threats and vulnerabilities to these systems, and provides recommended security countermeasures to mitigate the associated risks.

- 800-82 Rev 1 was released May 2013 - has 800-53 Rev 3 Appendix I controls
- 800-82 Rev 2 is scheduled for release spring 2014 - will have 800-53 Rev 4 controls

CNSSI 1253 ICS Overlay v1


Committee on National Security Systems Instruction
(CNSSI) No. 1253

SECURITY CONTROL OVERLAYS
FOR
INDUSTRIAL CONTROL SYSTEMS
Version 1
January 2013

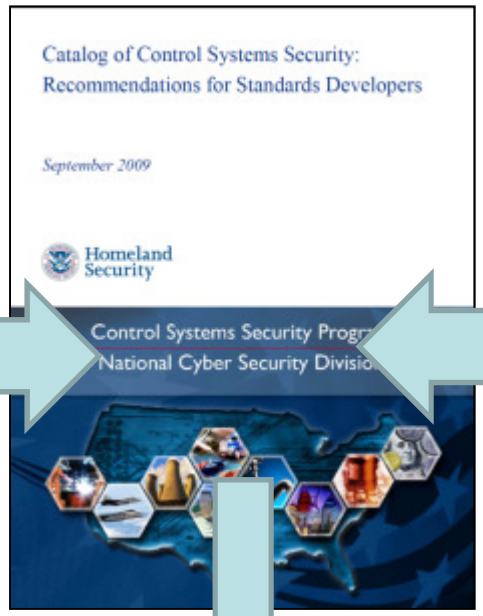


- ***V1 = DoD centric draft submitted to CNSS Jan '13; included DHS CSET 5.1***
- ***V2 = Removed DoD specific text, generalized for all CNSS members, model template for NIST 800-82 Rev 2, final in progress; planned for CSET 6.1***
- ***Defines a standard architecture, pictorial of components / devices***

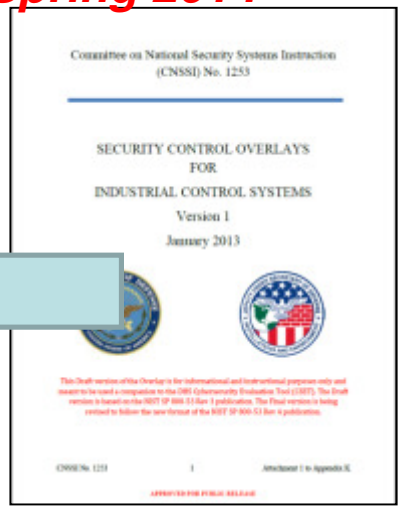
NIST SP 800-53 and SP 800-82

800-53 Rev 4 April 30, 2013

800-82 Rev 2 Spring 2014



CNSSI 1253 ICS Overlay v2 Spring 2014



DHS Control Systems Catalog

		AGA12-1	AGA12-2	FIPS 140-2	API 1164	Security Guidelines for the Petroleum Industry	CIDX	ISO 17799	ISO 27001	IEC 62351	IEEE 1402	ISA99-1	ISA99-2	NERC Security Guidelines	NERC CIP-2	NIST SP800-53 Rev 3
2.1.1	Security Policy and Procedures	X	—	X	X	X	X	X	X	—	—	X	X	—	X	X
2.2.1	Management Policy and Procedures	—	—	—	X	—	X	X	X	—	—	X	X	—	X	X
2.2.2	Management Accountability	X	—	—	X	—	X	X	X	—	—	X	X	—	X	X
2.2.3	Baseline Practices	—	—	—	X	—	X	X	X	—	—	X	X	—	—	—
	Coordination															

Update to NIST SP 800-82 Rev 2, CNSSI 1253, ISC CVS

Operational Technology (OT)

	Information Technology	Operational Technology
Purpose	Process transactions, provide information	Control or monitor physical processes and equipment
Architecture	Enterprise wide infrastructure and applications (generic)	Event-driven, real-time, embedded hardware and software (custom)
Interfaces	GUI, Web browser, terminal and keyboard	Electromechanical, sensors, actuators, coded displays, hand-held devices
Ownership	CIO, IT	Engineers, technicians, operators and managers
Connectivity	Corporate network, IP-based	Control networks, hard wired twisted pair and IP-based
Role	Supports people	Controls machines

OT Control System Components

Looks like IT, but configured, operates, and uses different ports and services; HMI, AMI, Modbus, BACnet, DNP 3, LonWorks, Fox, Proxibus, etc

The Cyber Threat Against ICS

Stuxnet - the ballistic missile of ICS warfare

Duqu - malware looks for information that could be useful in attacking industrial control systems

Flame - malware looks for engineering drawings, specifications, and other technical details about the systems and records audio, screenshots, keyboard activity and network traffic

Shamoon - destroyed over 30,000 Saudi Armco work stations

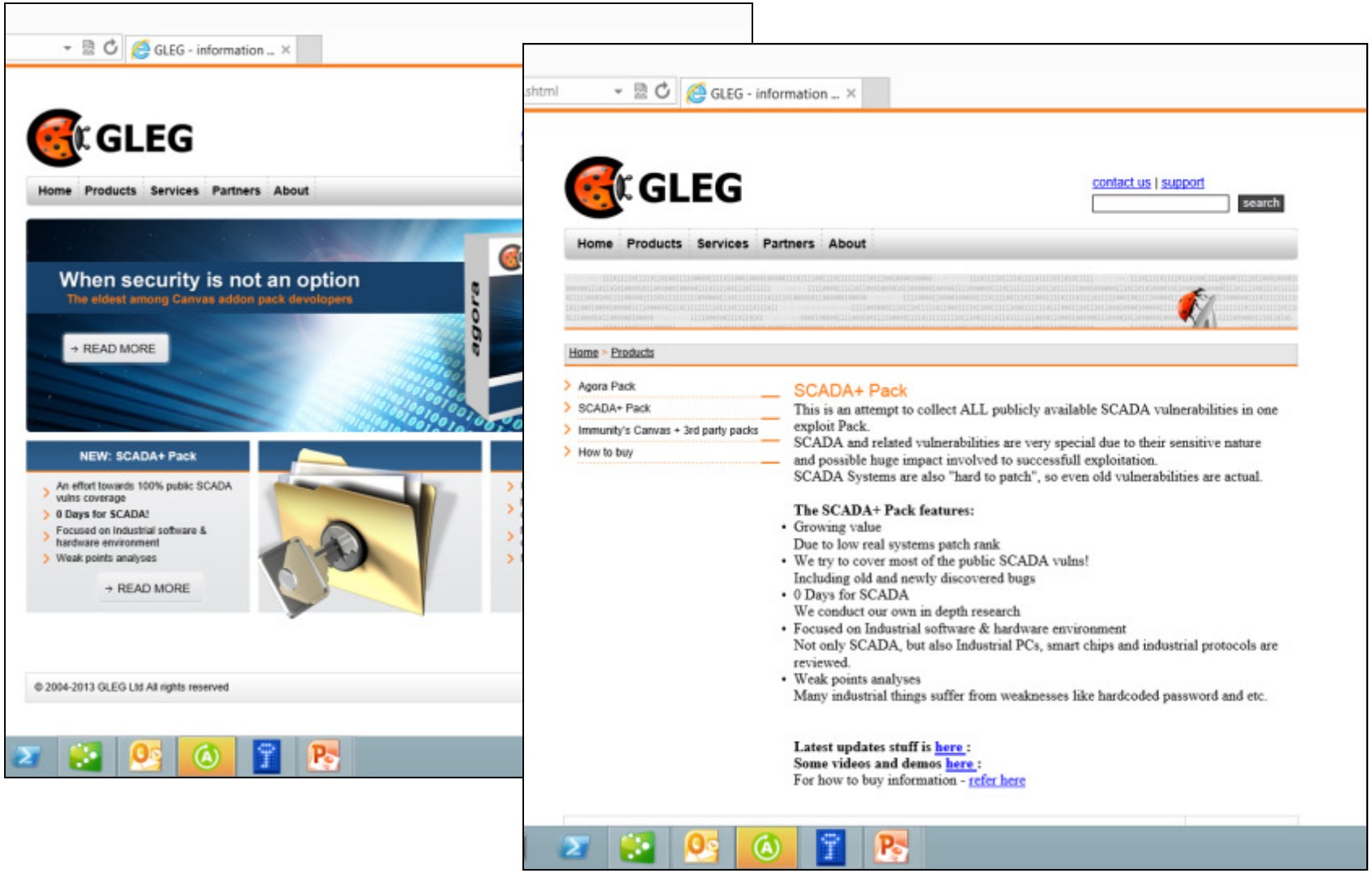
The Shamoon malware has the ability to overwrite the master boot record of a computer. Image credit: Securelist

Bits and bytes can now be used to physically destroy, spoof, or disrupt every sector of CI

Shodan


http://www.shodanhq.com/
Who's viewed your pro...
MSN
SHODAN - Comput...
Main
Exploits
Research
Videos
Anniversary Promotion
Register
Login
SHODAN
Search
EXPOSE ONLINE DEVICES.
WEBCAMS. ROUTERS.
POWER PLANTS. IPHONES. WIND TURBINES.
REFRIGERATORS. VOIP PHONES.
TAKE A TOUR
FREE SIGN UP
Popular Search Queries: default password - Finds results with "defa
DEVELOPER API
Find out how to access the Shodan database with Python, Perl or Ruby.
IN THE PRESS
Shodan: a search engine for hackers
Hack Shodan Room & Idihaye
DefCon: Dan Tentler Discusses
hacking was never so easy with
Shodan: World's scariest search
System Shock 2 Look at you,
Shodan: un Google per
AUX::UTIL::SH...
WARGAM "System !
this movie clip is a tiny pice of what you can do on this site.
explore the site on your own.
hacking was never so easy with shodan hq...
3/2/2012
you are now the inurl searches for webcams, printers, etc Sat also because these yield little look at shodanhq
http://www.youtube.com/watch?v=BvEtcWuFoiA
Related Searches
YouTube Hacking Lazers
YouTube Hacking
Hacking Parody
How To Hack YouTube
YouTube Hackers
How To Hack Everything
YouTube Hacking
Hack A YouTube
Links
9:09 AM
7/1/2013

Gleg

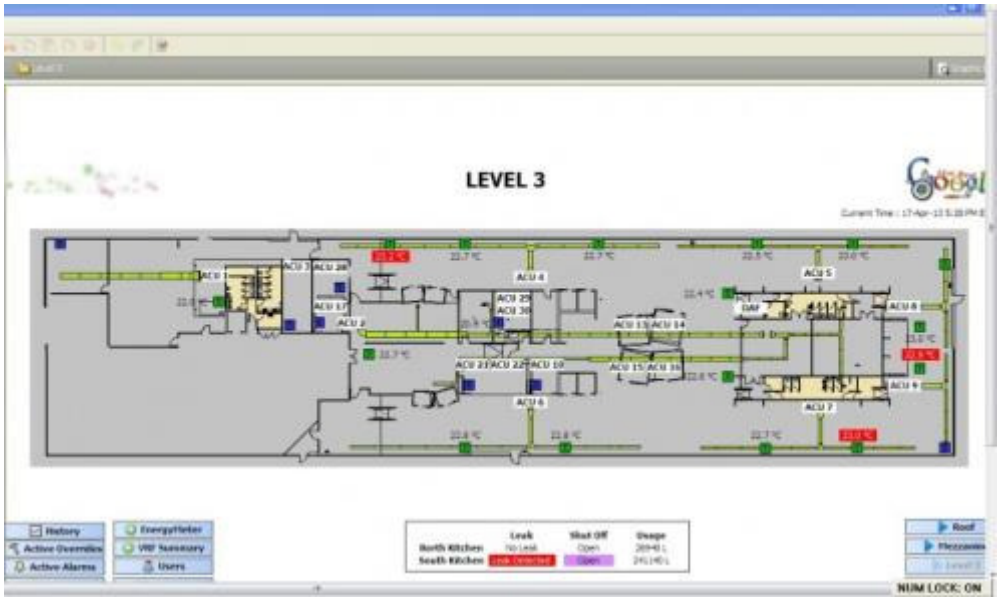


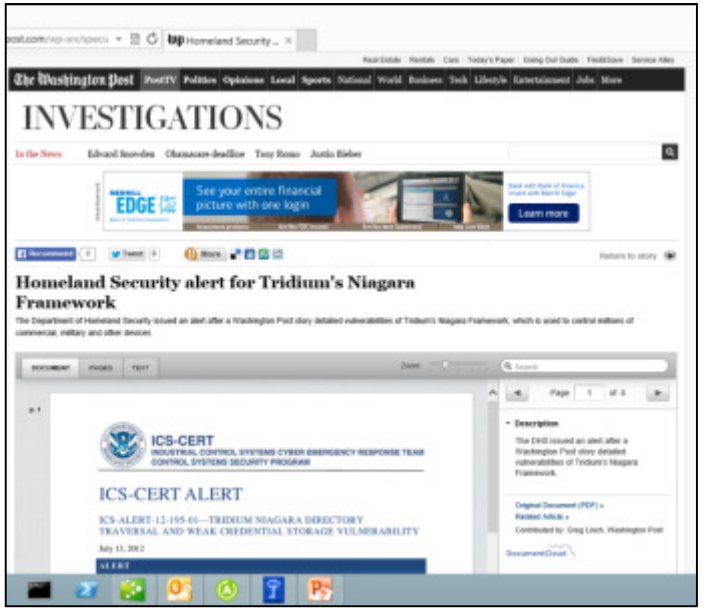
Exploits written specifically for SCADA

Building Automation Systems

Washington Post - Tridium's Niagara Framework: Marvel of connectivity illustrates new cyber risks

Researchers Hack Building Control System at Google Australia Office



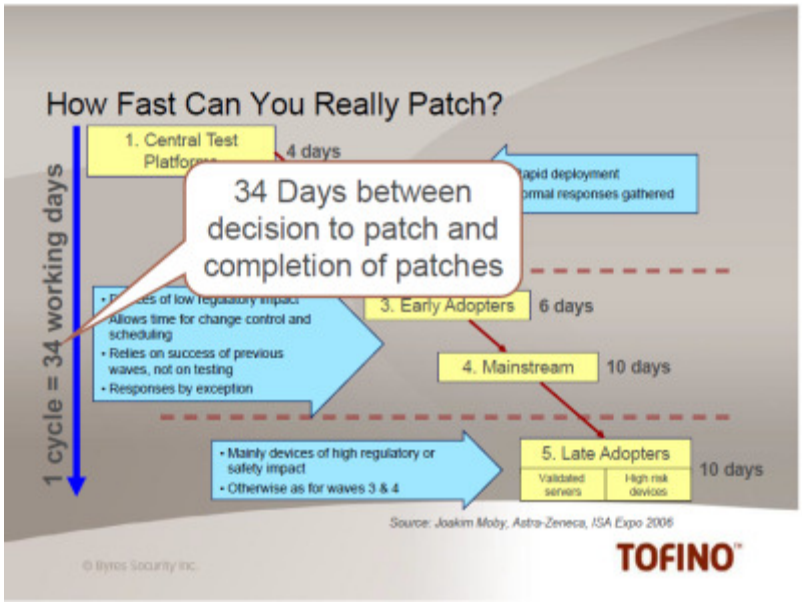


Google Australia uses a building management system that's built on the Tridium Niagara AX platform. Although Tridium has released a patch for the system, Google's control system was not patched.

ICS Vulnerabilities, Patching, Scanning

ICS must typically always remain in the “On” position

- Electric grid cannot deenergize
- Water mains cannot depressurize
- Cascading failures
- Must patch IT OS and Vendor OT
- Unintended consequences; printer auto searches for IP addresses
- Scanning overwhelms devices (8 bits); DOS



Oh Boy! I can print in color..what is color?

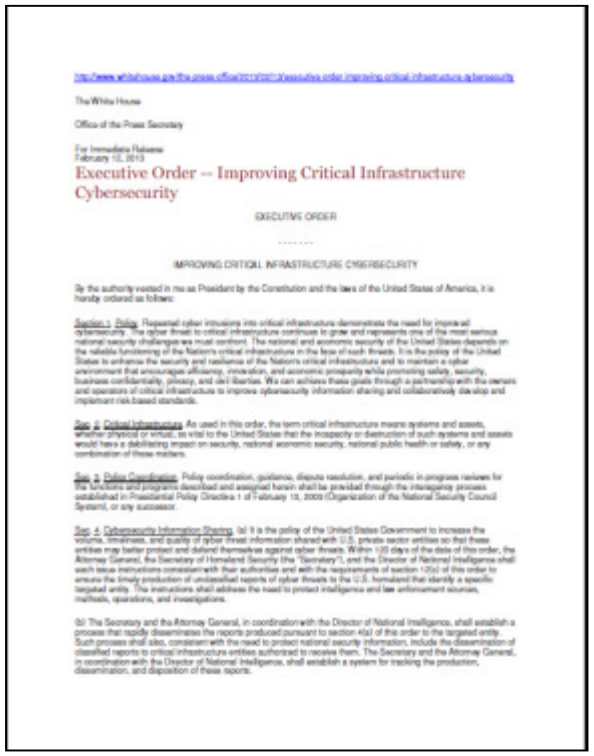
Patches, continuous monitoring and scanning can break OT

Security of IT Versus OT

SECURITY TOPIC	IT	OT
Anti-virus & Mobile Code Countermeasures	Common; Widely Used	Uncommon; Difficult to Deploy
Support Technology Lifetime	3-5 Years	Up to 20 Years (or Longer)
Outsourcing	Common; Widely Used	Rarely Used
Application of Patches	Regular/Scheduled	Slow (Vendor Specific)
Equipment Refresh	Regular/Scheduled	Legacy Based; Unsuitable for Modern Security
Time Critical Content	Delays are Generally Accepted	Critical Due to Safety
Availability	Delays are Generally Accepted	24x7x365 (Continuous)
Security Awareness	Good in Both Private and Public Sectors	Generally Poor Regarding Cyber Security
Security Testing/Audit	Scheduled and Mandated	Occasional Testing for Outages
Physical Security	Secure	Very Good, But Often Remote and Unmanned

There will be new workforce training and education required, new contract and procurement language, new assessment and management roles

Executive Orders – CI and Cyber



The White House

Office of the Press Secretary

For Immediate Release
February 12, 2013

Executive Order -- Improving Critical Infrastructure Cybersecurity

EXECUTIVE ORDER

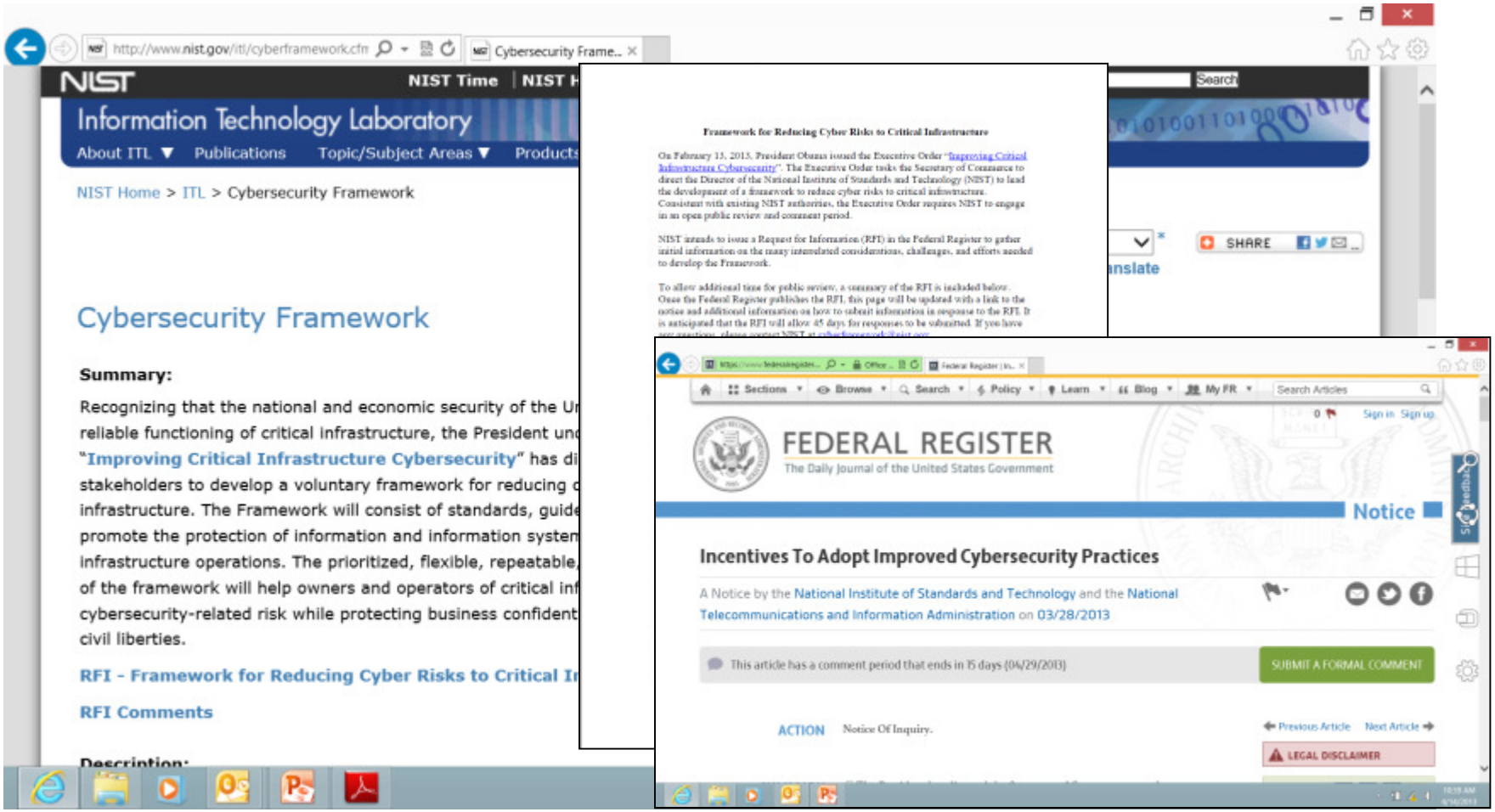
IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Sec. 7. Baseline Framework to Reduce Cyber Risk to Critical Infrastructure. (a) The Secretary of Commerce shall direct the Director of the National Institute of Standards and Technology (the "Director") to lead the development of a framework to reduce cyber risks to critical infrastructure (the "Cybersecurity Framework").

The Cybersecurity Framework shall include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks.

NIST Cybersecurity Framework



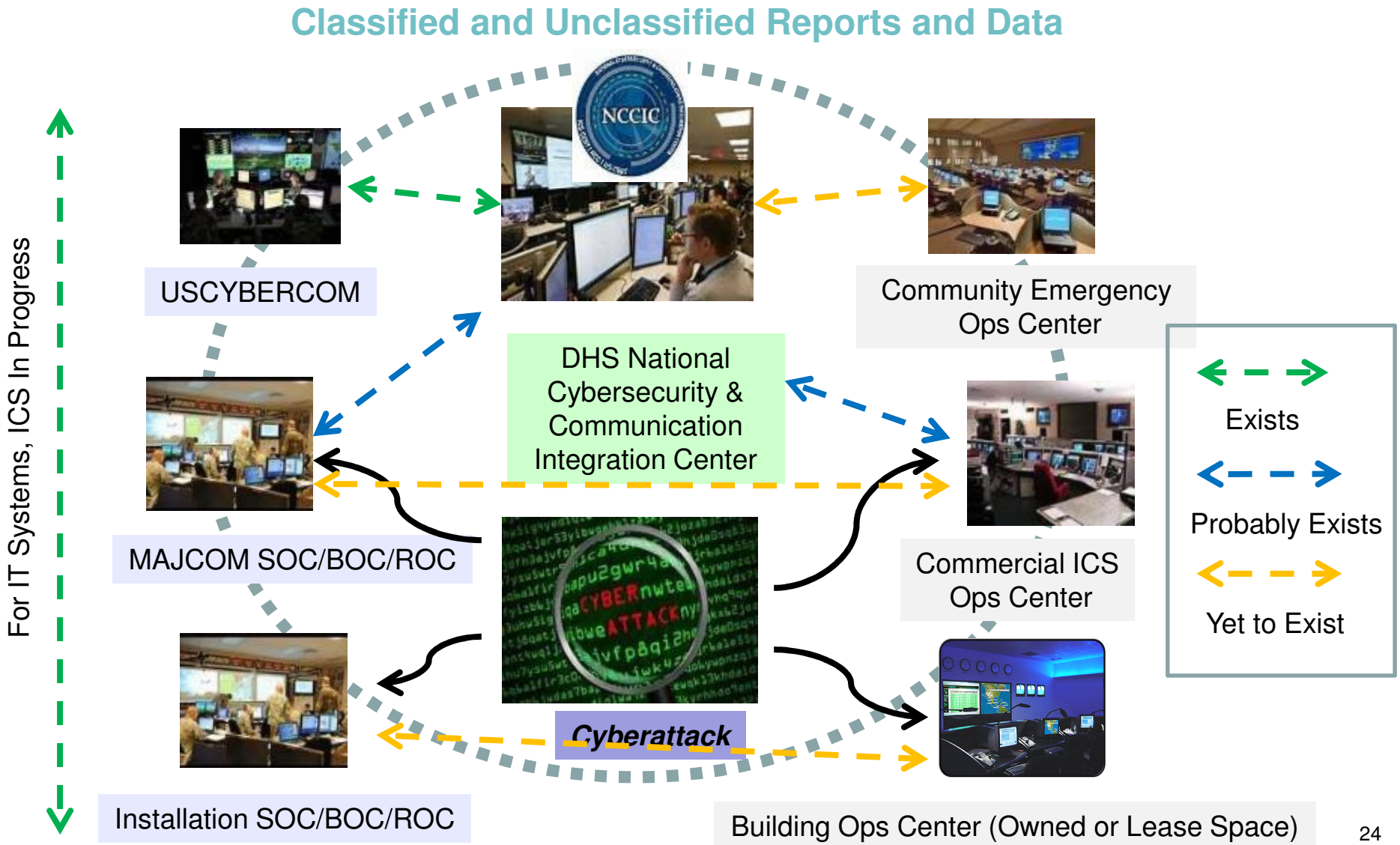
http://www.nist.gov/itl/cyberframework.cfm

Executive Order -- Improving Critical Infrastructure Cybersecurity Sec 4

Sec. 4. Cybersecurity Information Sharing. (a) It is the policy of the United States Government to increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities so that these entities may better protect and defend themselves against cyber threats. Within 120 days of the date of this order, the Attorney General, the Secretary of Homeland Security (the "Secretary"), and the Director of National Intelligence shall each issue instructions consistent with their authorities and with the requirements of section 12(c) of this order to ensure **the timely production of unclassified reports of cyber threats to the U.S. homeland that identify a specific targeted entity.** The instructions shall address the need to protect intelligence and law enforcement sources, methods, operations, and investigations.

(b) The Secretary and the Attorney General, in coordination with the Director of National Intelligence, shall establish a process that rapidly disseminates the reports produced pursuant to section 4(a) of this order to the targeted entity. **Such process shall also, consistent with the need to protect national security information, include the dissemination of classified reports to critical infrastructure entities authorized to receive them.** The Secretary and the Attorney General, in coordination with the Director of National Intelligence, shall establish a system for tracking the production, dissemination, and disposition of these reports.

Conceptual Information Sharing



DHS NCCIC and ICS-CERT

National Cybersecurity and Communications Integration Center
http://www.us-cert.gov/nccic/

NIST 800-30

NIST 800-53 Rev 3

NIST 800-53 Rev 4

NIST 800-82 Rev 1

NIST 1108

NISTR 7628

CNSSI 1253 ICS Overlay

NERC CIP

DHS CSET 5.1

DHS CSET 6.0 (Jan 2014 release)

NIST SP 800-53 Rev 4 and 800-82 Rev 2

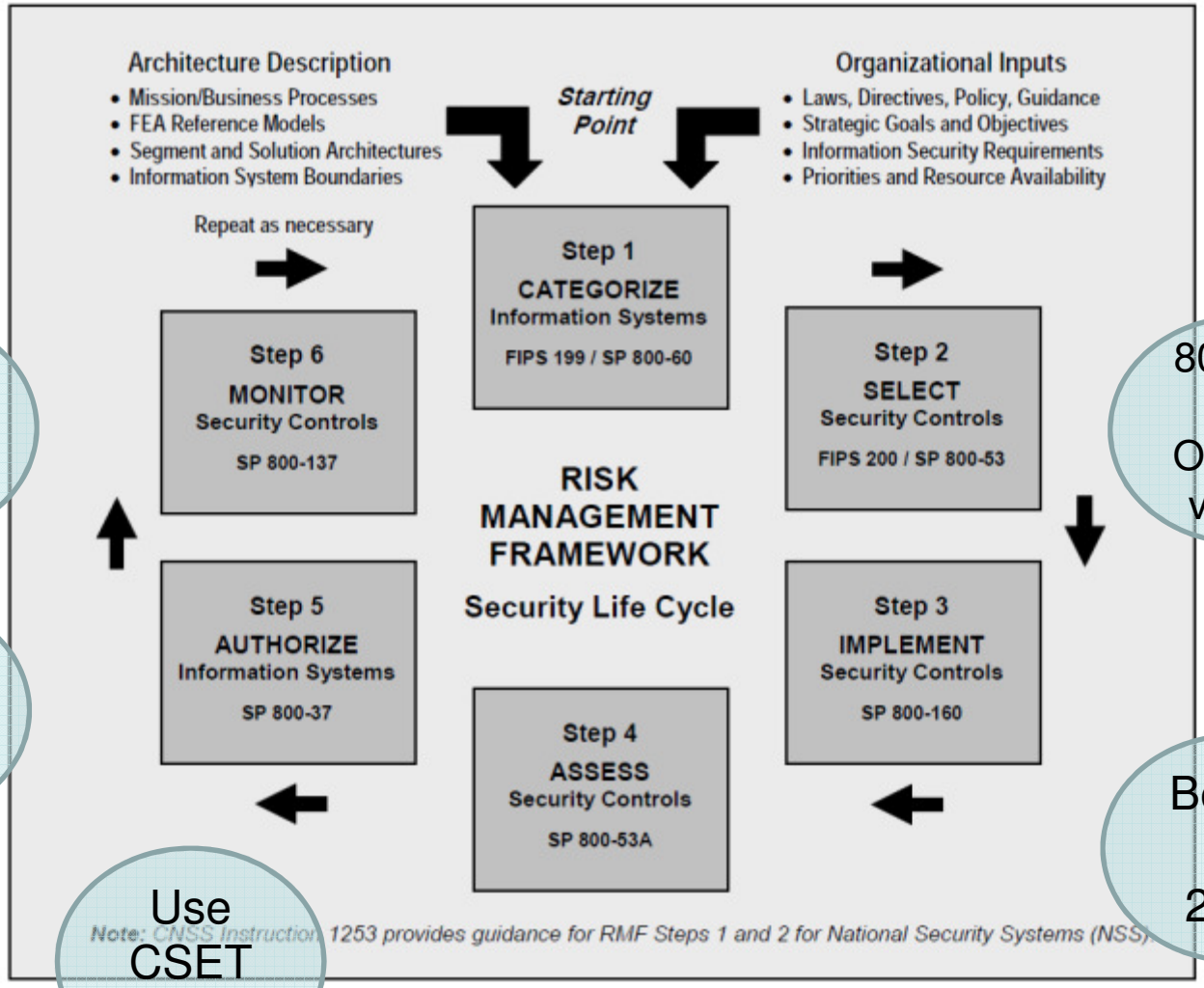


FIGURE 2: RISK MANAGEMENT FRAMEWORK

2015?

Initial ATO's 2014?

Use CSET Tool

800-82, ICS Overlay v1, v2

Began in 2013

NIST SP 800-82 Rev 2 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

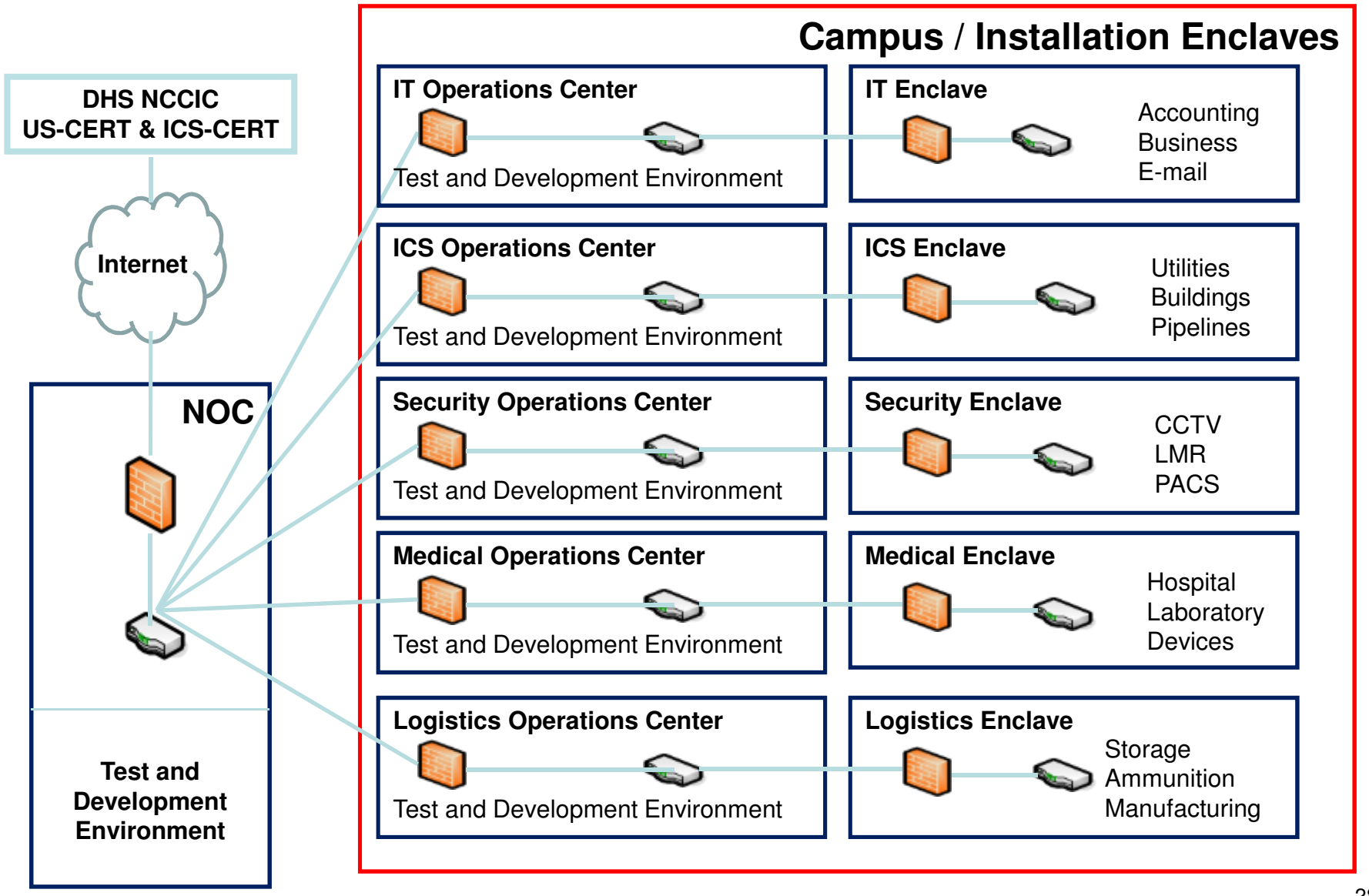
Test and Development Environment
- CA-8 Penetration Testing
- CM-4 Security Impact Analysis
- CP-3 Contingency Training
- CP-4 Contingency Plan Testing and Exercises
- PM-14 Testing, Training and Monitoring

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

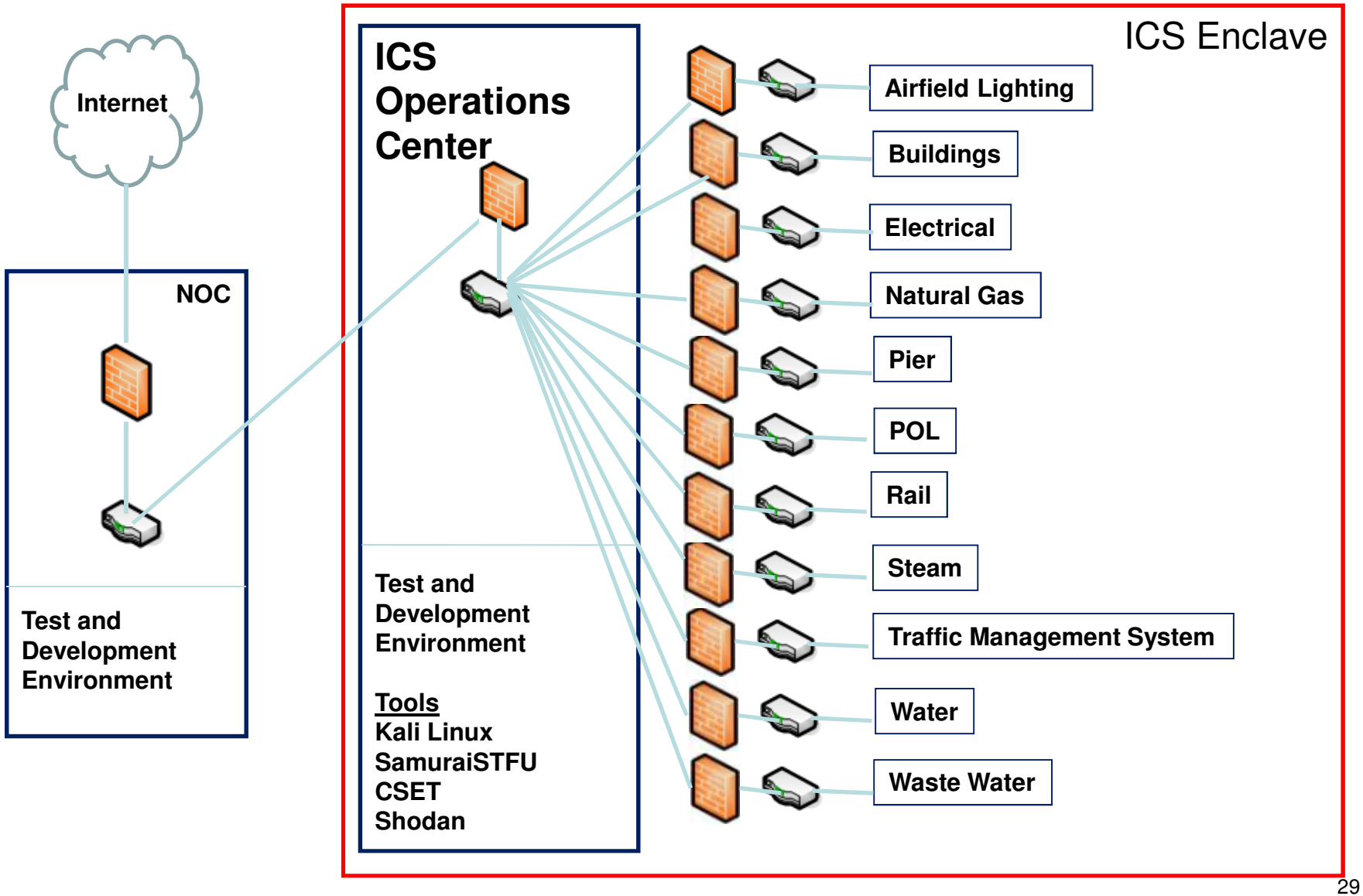
Acquisition and Contracts
- AU-6 Audit Review, Analysis, and Reporting
- CA -7 Continuous Monitoring
- SA-4 Acquisitions
- PM-3 Information System Resources
- PM-14 Testing, Training and Monitoring

Inbound Protection, Outbound Detection

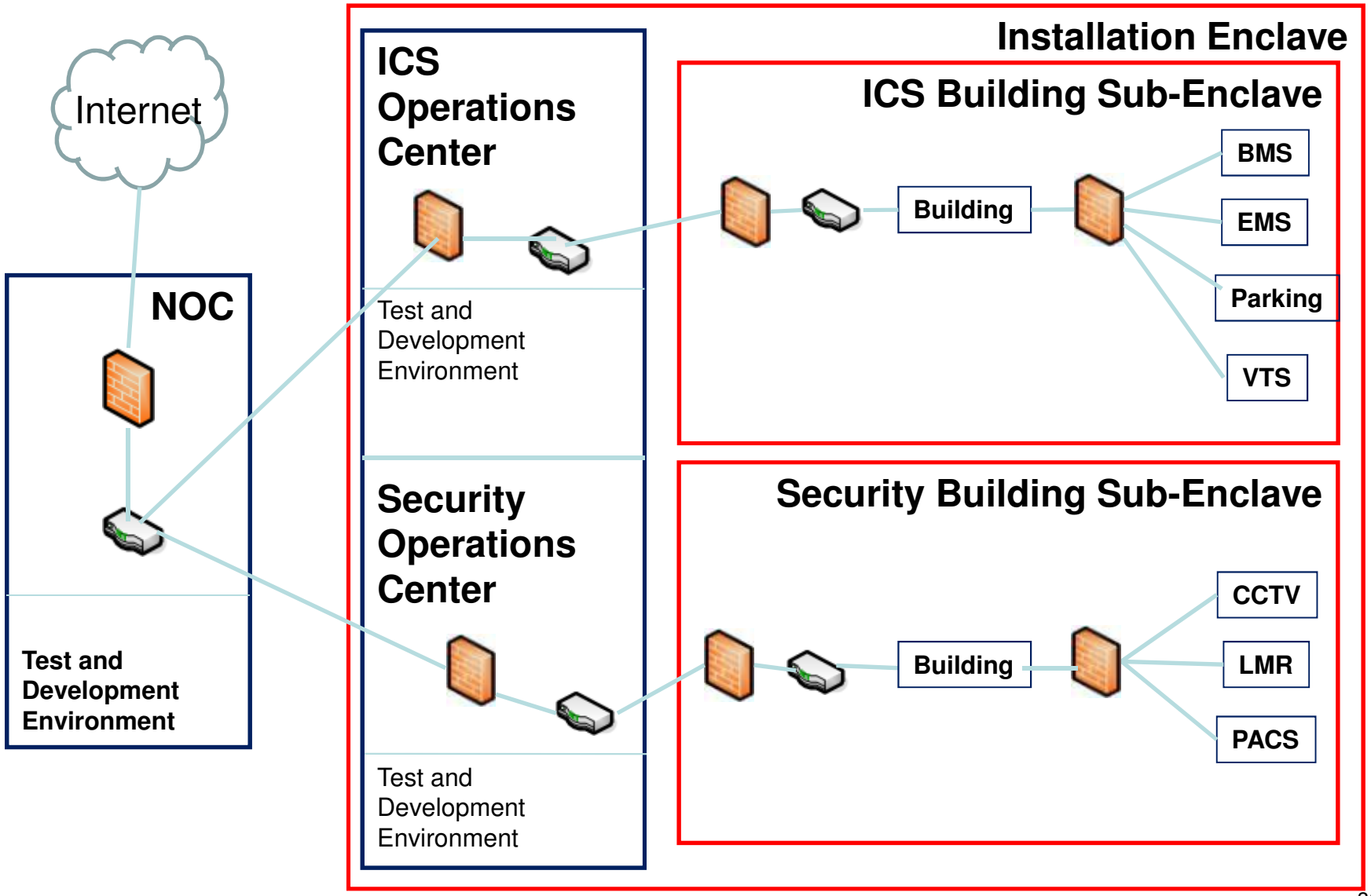
Campus / Installation Enclaves



Numerous ICS Sub-Enclaves



Hybrid ICS & Security Sub-Enclaves

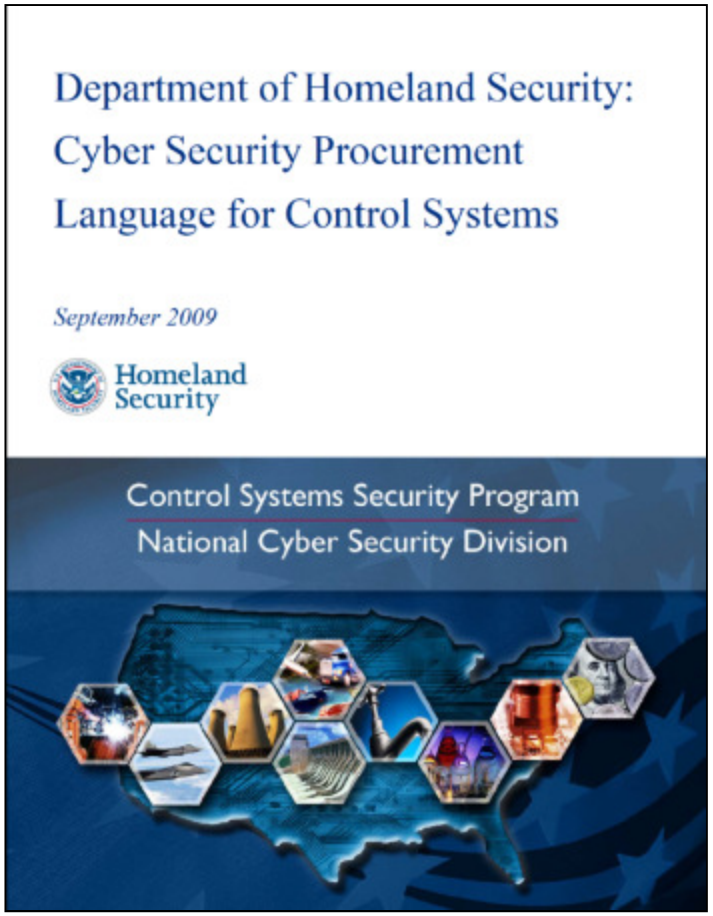


Draft DHS ISC White Paper

Activity	Description	Completion
Stand Up Development and Test Environments	Establish development and testing environments so that PACS developers and testers can conduct build activities in an environment that does not impact the agency's production systems.	4 – 6 weeks
Build/Configure Servers	Build and/or configure servers to properly operate the PACS solution, as needed based upon the chosen implementation path.	1 – 2 weeks
Install Supporting Software	Install supporting software (i.e., Commercial Off-The-Shelf [COTS] Identity Access Management [IAM] Suite) on PACS servers, as needed based upon the chosen implementation path.	1 – 2 weeks
Configure Supporting Software	Configure PACS software to specifically meet the agency's unique needs and/or perform certain functions, as needed based upon the chosen implementation path.	1 – 2 weeks
Implement and Assess Security Controls	Conduct Steps 3 and 4 of the Risk Management Framework (RMF) by applying the controls identified in the requirements and design phase and by assessing the adequacy and effectiveness of the security controls and documenting the findings in an assessment report.	12 – 20 weeks
Conduct Testing on Initial Build	Perform testing on the PACS solution in a development and/or test environment to ensure that system errors are found and corrected before the solution is deployed on the agency's network.	2 – 4 weeks
Conduct Pilot Implementation Deployment	Conduct a pilot implementation to expose a small subset of the agency's user base to the PACS solution for the purpose of evaluating the solution's operations against real-world requirements.	Varies on size of deployment (number of facilities and

DRAFT

DHS ISC Procurement Language



Planning and Design

- 90% design complete initial CSET evaluation
- Apply hardening criteria (e.g. DoD STIGS)
- Conduct initial Penetration Testing

Construction (e.g. SamuraiFTSU)

- 50-75% construction complete conduct Factory Acceptance Testing (FAT) of major components
- 100% construction complete conduct Site Acceptance Testing (SAT)
- Conduct Penetration Testing
- Create System Security Plan (SSP)
- Create Plan of Action and Milestones (POAM)

DHS ISC Procurement Language Example

1.0 SYSTEM HARDENING

System hardening refers to making changes to the default configuration of a network device and its operating system (OS), software applications, and required third-party software to reduce system security vulnerabilities.

1.1 FAT Measures

The Vendor shall verify that the Purchaser requires the results of cyber security scans (as a minimum a vulnerability and active port scan, with the most current signature files) run on the control system as a primary activity of the FAT. This assessment is then compared with an inventory of the required services, patching status, and documentation, to validate this requirement.

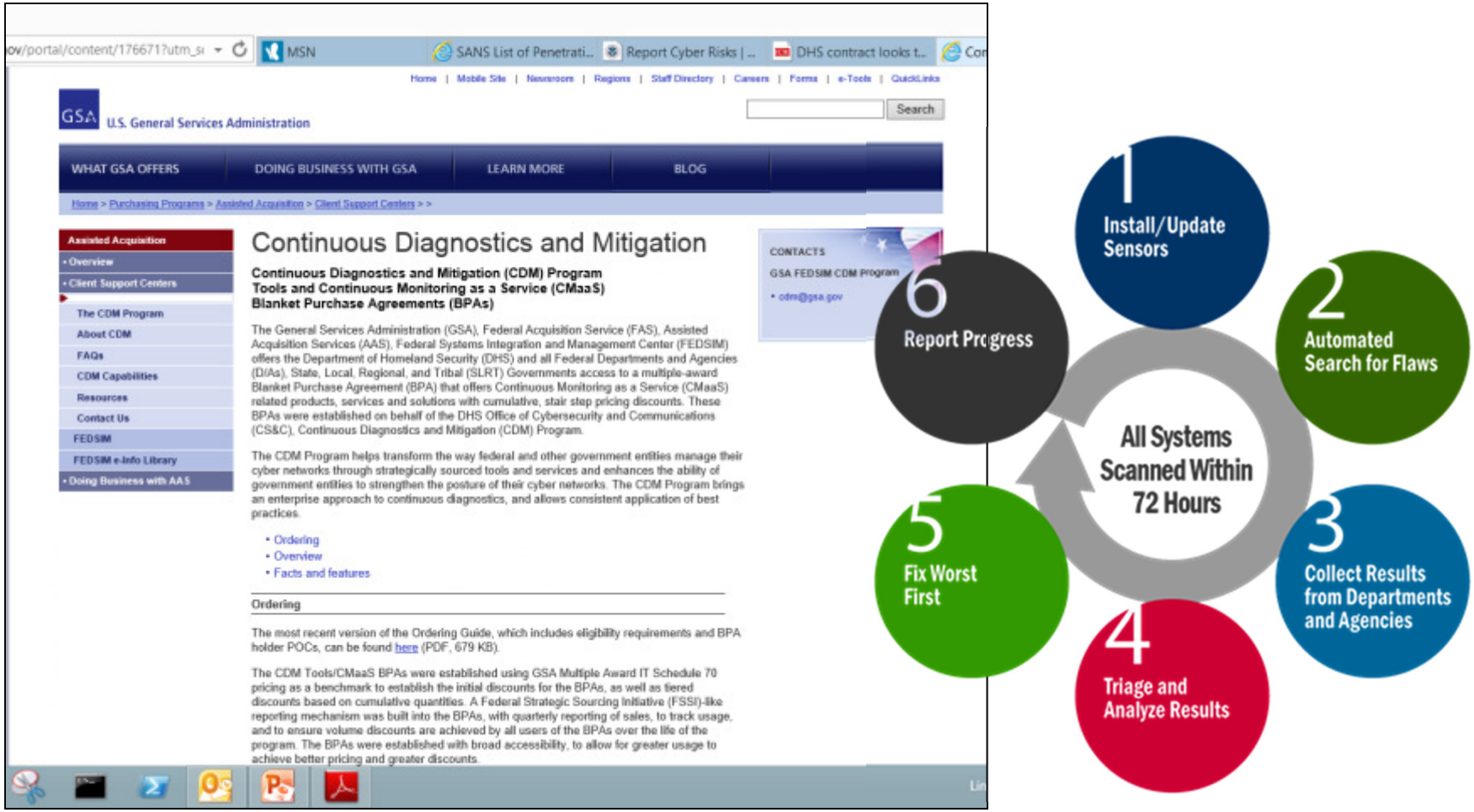
1.2 SAT Measures

The Vendor shall compare the results of cyber security scans run on the system, as a primary activity of the SAT, with an inventory of the required services, patching status, and required documentation. At the conclusion of the SAT and before cutover or commissioning, the above cyber security scans (with the most current signature files) must be run again.

1.3 Maintenance Guidance

Document the system operating system and software patches as the system software evolves to allow traceability and to verify no extra services are reinstalled. Anytime the system is upgraded, it is recommended that system Vendors rerun appropriate subsets of the FAT on the baseline system before delivery to the purchaser.

DHS Continuous Diagnostics and Mitigation



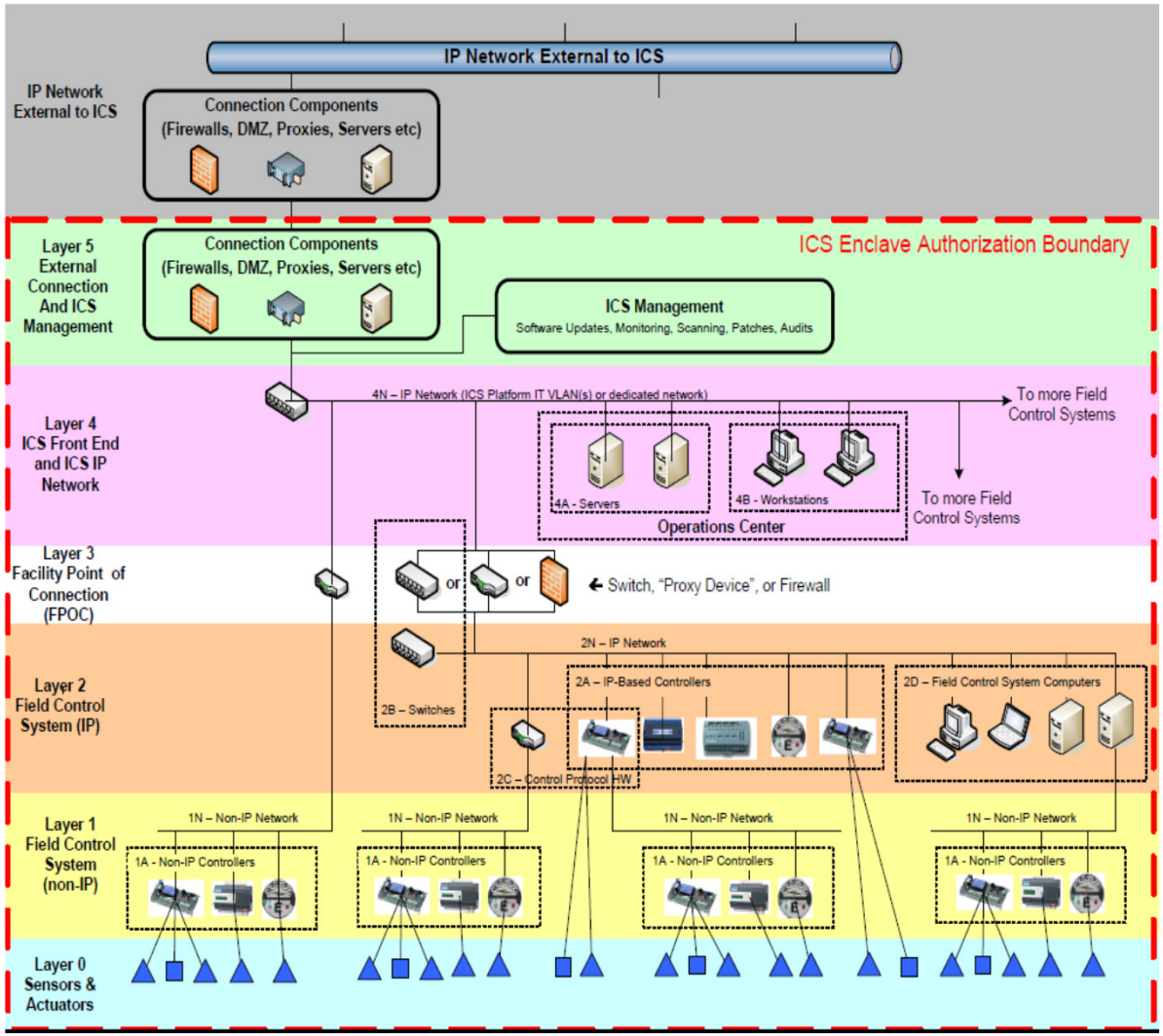
http://www.gsa.gov/portal/content/176671?utm_source=FAS&utm_medium=print-radio&utm_term=cdm&utm_campaign=shortcuts

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

- Undocumented connections
- Lack of encryption / clear text
- Difficult patch management
- Lack of authentication
- Limited logging & monitoring
- Lack of segmentation
- Hardcoded passwords & defaults
- Lack of application security
- Limited access control
- Third party software
- Protocol weaknesses

© 2014 NexDefense, Inc.

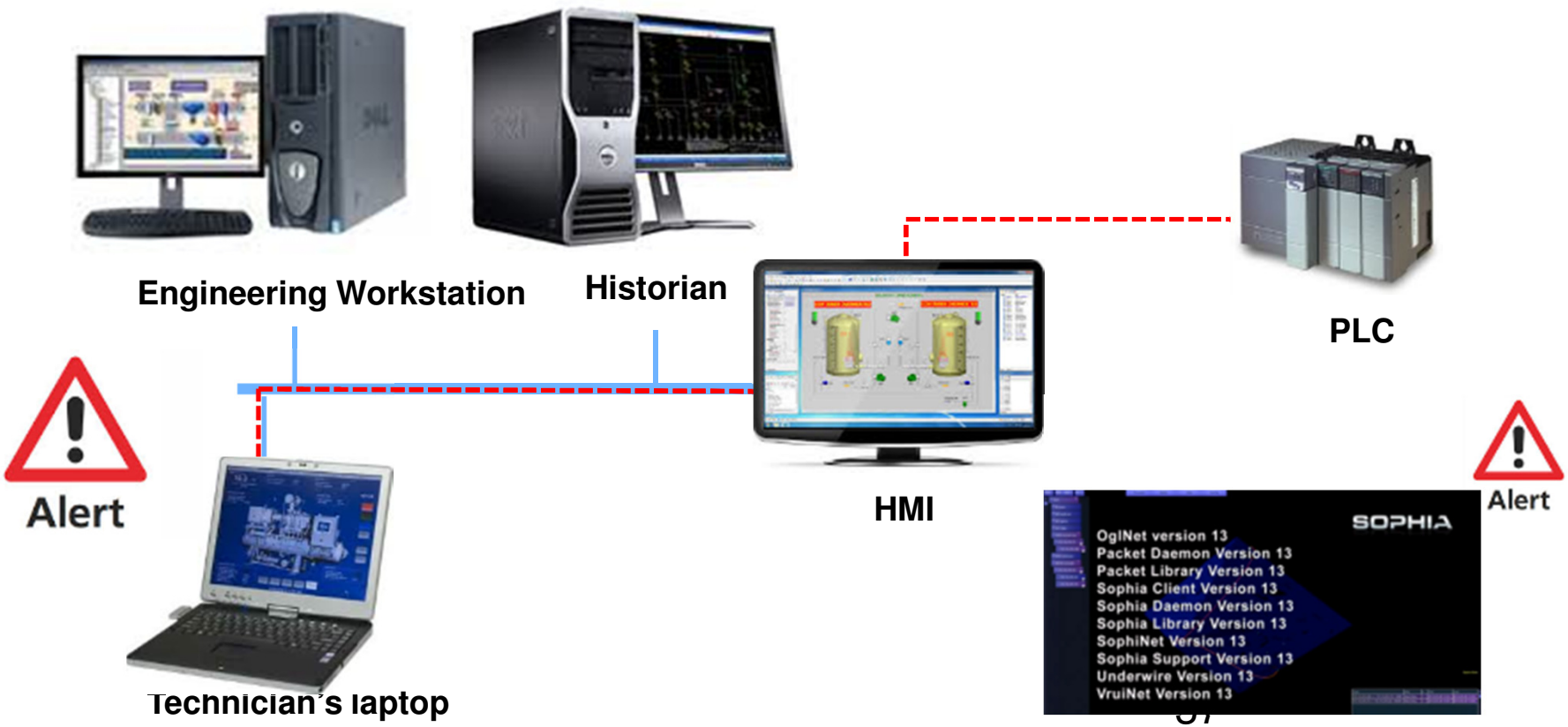
ICS/SCADA Fingerprinting And Monitoring Tool

Passive, real time tool for interdevice communication discovery and monitoring of the active elements in a ICS/Supervisory Control and Data Acquisition (SCADA) system.

- Developed at Idaho Nat'l Labs (3 years, $1.5M from DOE)
- Beta-tested by over 40 organizations
- In use by 7 US government depts (DHS, Army, Navy, etc.)
- Exclusive commercialization license to NexDefense

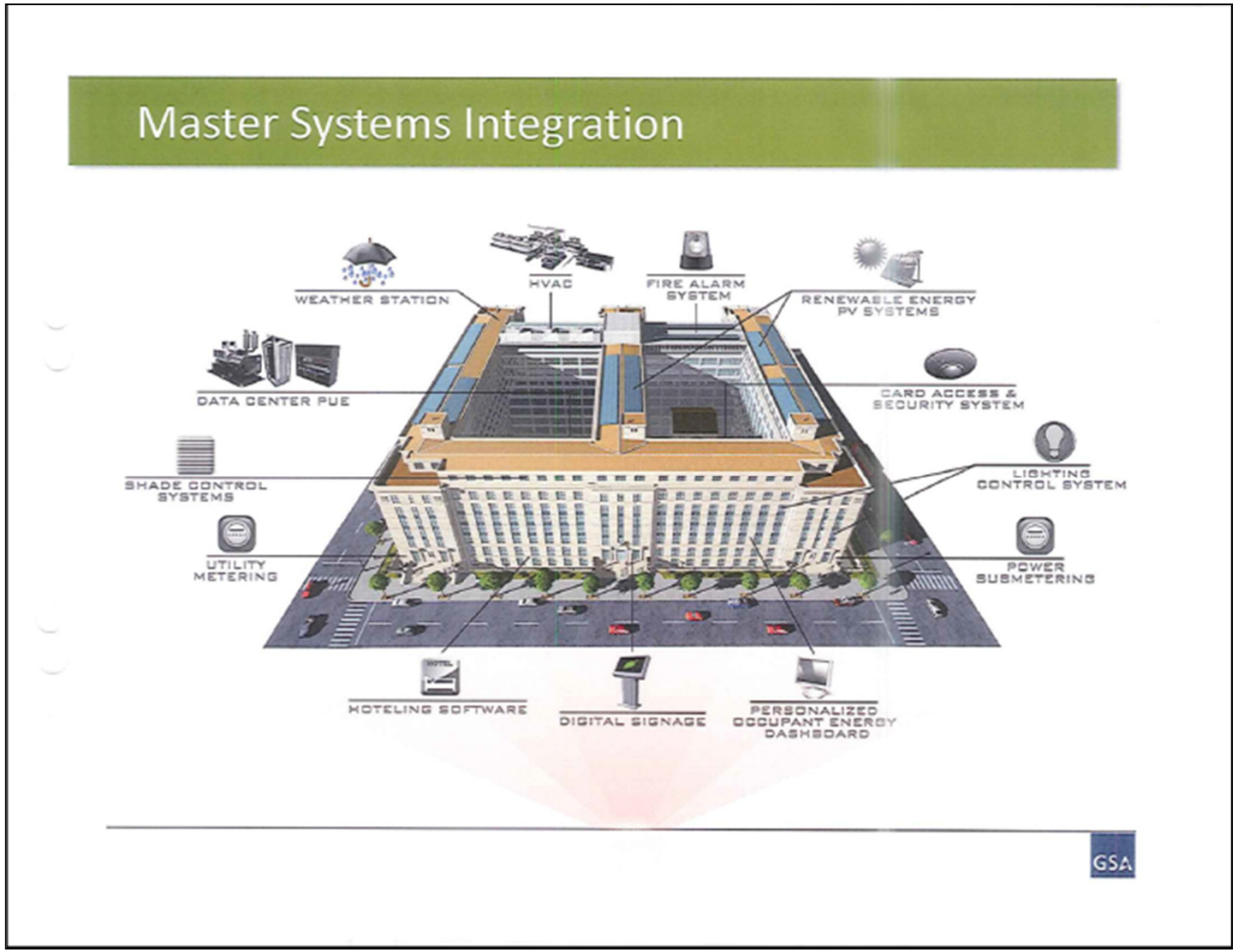
Sophia

- Sophia can baseline approved/expected communication behavior
- Alert on communication sessions that are suspect/unexpected
- Example: DB Technician laptop should never send a Modbus command to the PLC



GSA Smart Buildings Sources Sought

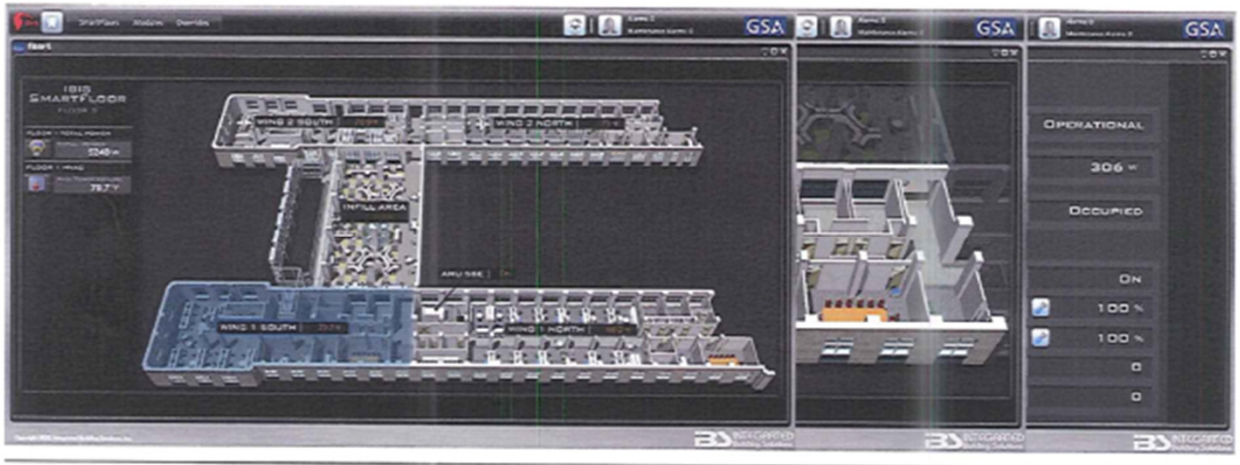
GSA Smart Buildings Sources Sought



GSA Smart Buildings Sources Sought

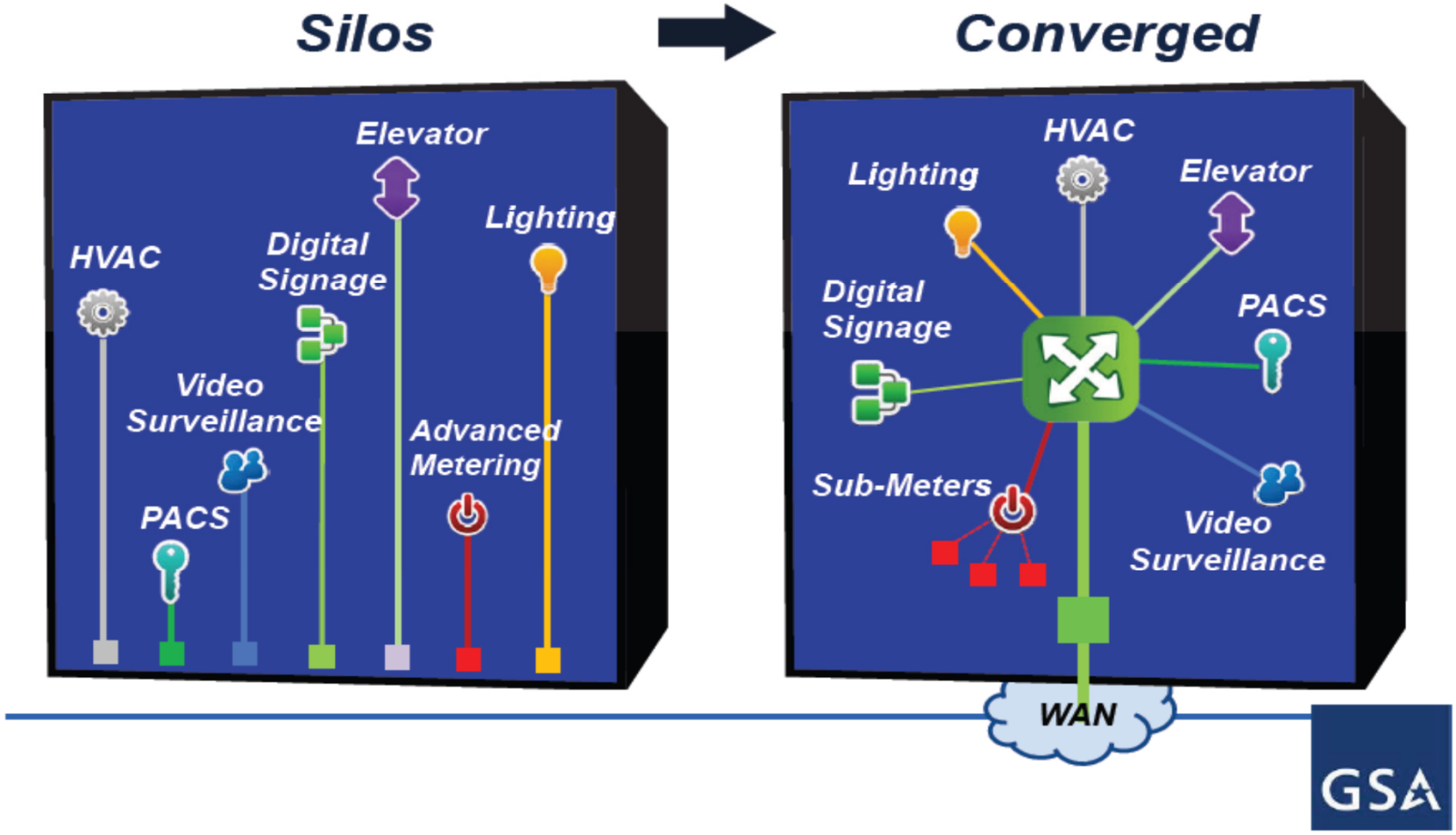
Security & Card Access / Fire Alarm

- **Security & Card Access Brivo Integration** – Primary Monitoring, Alarming and Trending
  - Monitor Status and Alarm for primary security equipment
  - Activate Floor lights where Security Event is active (Door Ajar, Forced Entry, AC Power Loss)
  - Occupant Head Count (Energy Metrics Per Person)
  - Automatic Check in for "Book It" Reservations
- **Fire Alarm** – Primary Monitoring, Alarming and Trending
  - Turn on all lights in the building when in Fire Mode



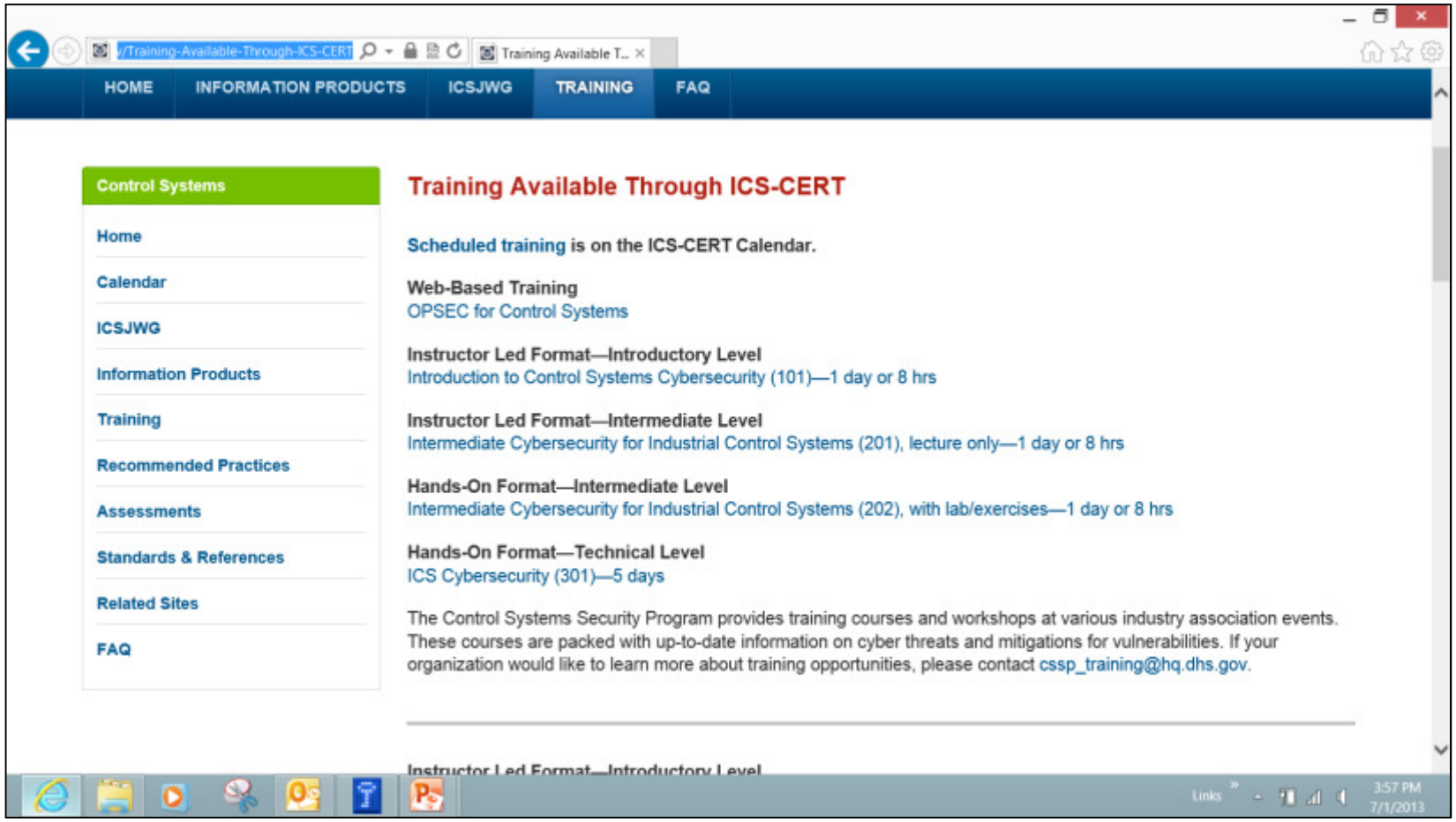
GSA

GSA Smart Buildings



CIO provides routers, switches and firewalls, OT connects in distribution closet

DHS ICS-CERT Training



https://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT

SANS ICS 410 – ICS Security Essentials

- The SANS Industrial Control Systems Team is working to develop a curriculum of focused ICS courseware to equip both security professionals and control system engineers with the knowledge and skills they need to safeguard our critical infrastructures. The entry level course in the SANS ICS Curriculum is ICS 410 – ICS Security Essentials
- This course provides students with the essentials for conducting security work in Industrial Control System (ICS) environments. Students will learn the language, the underlying theory and the basic tools for ICS security in industrial settings across a diverse set of industry sectors and applications. This course will introduce students to ICS and provide the necessary information and learning to secure control systems while keeping the operational environment safe, reliable, and resilient.

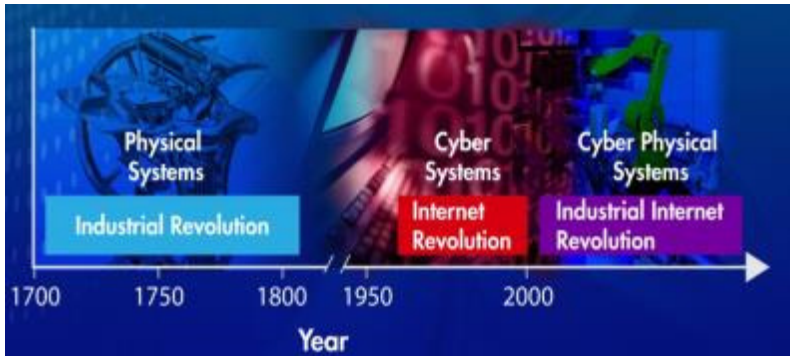
SANS GICSP

- SANS GIAC is developing a vendor neutral, practitioner focused Industrial Control System certification. The Global Industrial Cyber Security Professional Certification (GICSP) will assess a base level of knowledge and understanding across a diverse set of professionals who engineer or support control systems and share responsibility for the security of these environments.
- This certification will be leveraged across industries to ensure a minimum set of knowledge and capabilities that an IT, Engineer, and Security professional should know if they are in a role that could impact the cyber security of an ICS environment.

NIST Cyber-Physical Systems Workshop

http://events.energetics.com/NIST-CPSWorkshop/index.html

Future - Industrial Internet Revolution



NY Times June 19, 2013

- General Electric Adds to Its 'Industrial Internet
- Cisco Systems is in the middle of an "Internet of Everyhing" strategy that involves selling software and services for a world rich in sensors
- Phillips is also offering data-gathering connectivity in both its health care and lighting products

FED iFM – Cloud Web Services and Apps

WBDG Cybersecurity Resource Page

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

WBDG FED iFM Resource Page

www.wbdg.org/fedifm

Summary

- Maintain Situational Awareness of the Cybersecurity Framework
- Prepare CIO and IT staff for new role scanning and protecting ICS systems
- Prepare Security, Engineering, Transportation and other ICS functions staff for new cybersecurity requirements
- Prepare the Acquisition and Contracting staff for new contract and procurement language
- Conduct pilot self-assessments of ICS using the CSET Tool, understand baseline, potential vulnerabilities, risks and mitigation measures
- Consider developing ICS Overlays for your organization (similar to the CNSSI 1253)
- Coordinate with DHS NCCIC, evaluate options for information sharing
- New skills to learn, new methods, but based on Risk