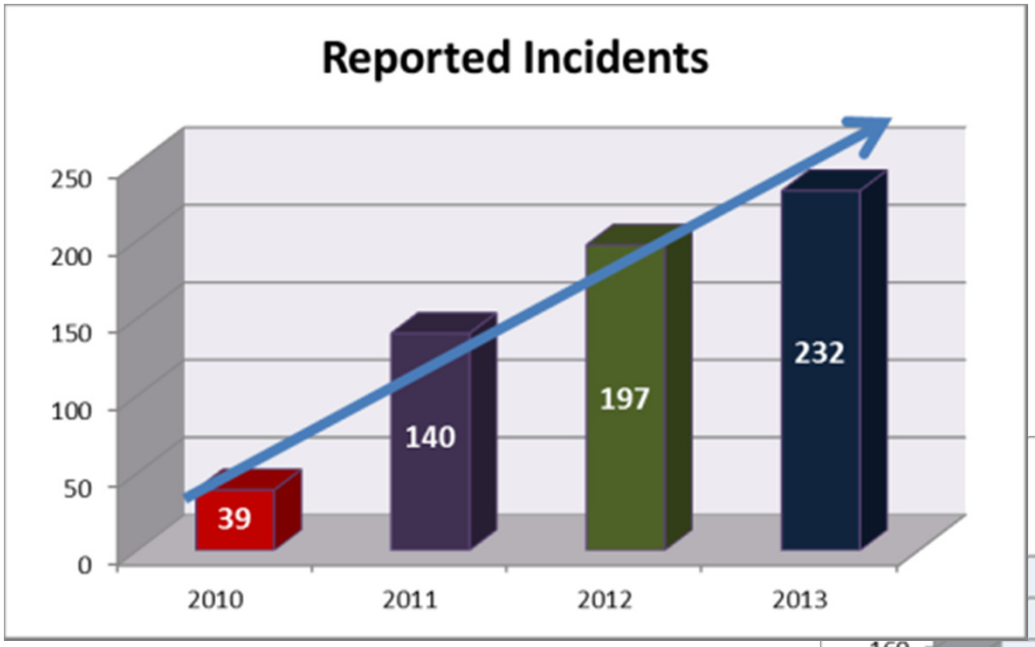
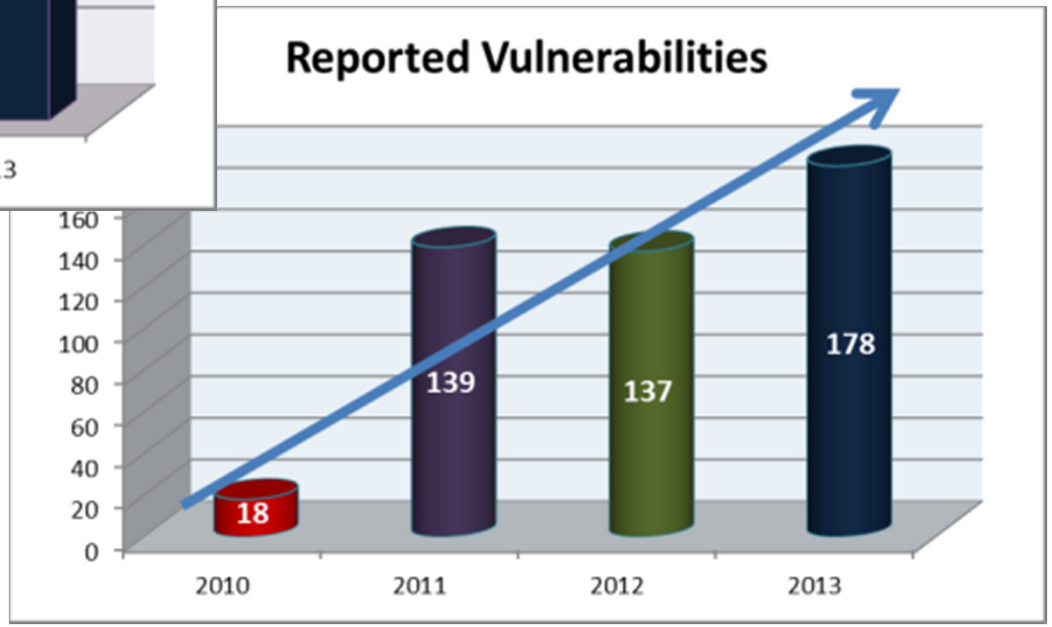
NIBS Cybersecurity Overview

Lisa Kaiser – Standards Chief
Control Systems Security / ICS-CERT

ICS-CERT Metrics





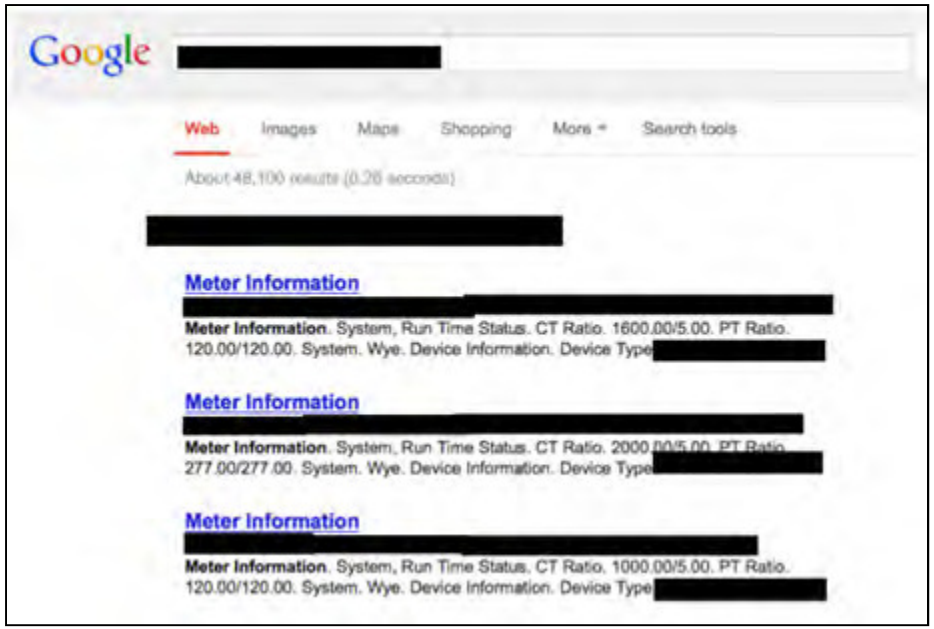
New Threat - Cyber Researchers

- Researchers who wear hats with a range of colors have all started paying attention to ICS vulnerabilities
- Researchers are developing an interest in SCADA systems and are increasing their work on control system vulnerabilities
- Researchers with no background in control systems have started looking at control system products and finding vulnerabilities

Searching isn't Easy?

- Internet facing control system devices are a **BAD** idea
- Locate control system networks and remote devices behind firewalls with improperly configured rules
- Default passwords are **BAD** change your passwords!
- Google-dorks can find embedded systems from as early as 2010

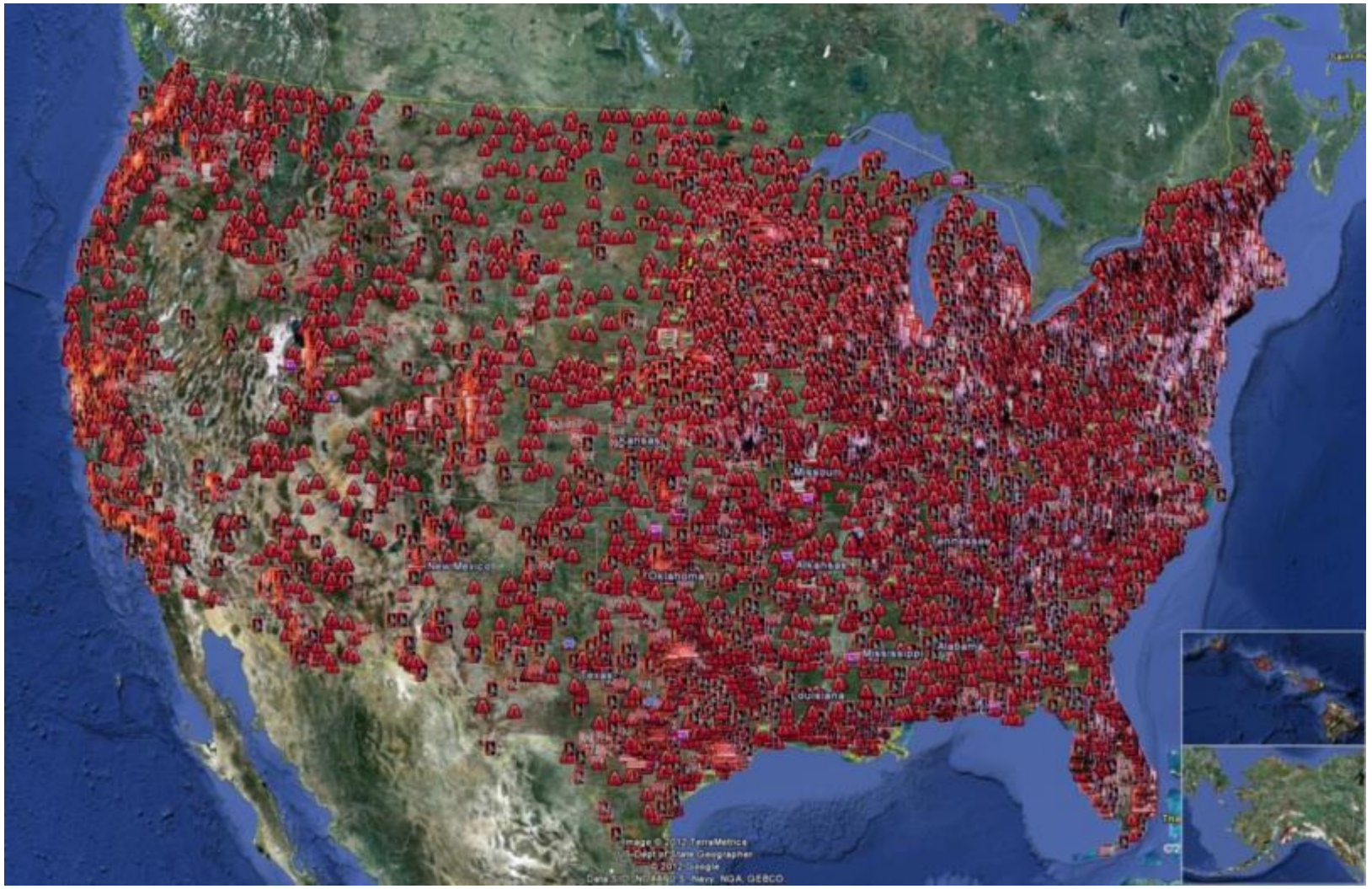
SHODAN
Computer Search Engine



RouterPasswords.com

default password list

98,000 Internet-Facing Devices



Homeland Security

DDoS Attacks Against Financial Sector

- Recent DDoS attacks against financial sector
  - Targeted public facing websites
  - Limited, but some impact
- Other sectors could make more interesting DDoS targets
  - Energy Markets (electricity/gas)
  - Medical records service providers
- Mitigations
  - Have a relationship with your upstream providers
  - DDoS mitigation services/technologies
  - Be mindful of all your core infrastructure (web, DNS, Email etc)

Targeted cyber attack on pipelines

- **23 targeted pipeline** operators (December 2011 – June 2012)
- **10 confirmed**, 3 near misses, 10 pending
- Adversary is targeting industrial control systems information
- Document searches: “SCAD*”
  - Personnel Lists
  - Usernames/Passwords
  - Dial-Up access information
  - System manuals
- Exfiltrated ICS access credentials
- The data exfiltrated could provide an adversary with the capability to access US ONG ICS including performing unauthorized operations

(U) What was taken?

- All_gate_meter.xls
- **<station>_SCADA 8-23-2002.vsd**
- Contact List Gas Scada.xls
- <redacted>_Area_RTUs.xls
- **Dial Up #### Vector Lists.xls**
- **SCADA_Server_UsersGuide.pdf**
- Gas Control Numbers.xls
- Gas SCADA Profiles Defined 10-22-03.xls
- Gas-Control Asset list.xls
- <station> Dialup.xls
- PASS1.xls
- <station> datapoints for log.xls
- RTU point list.xls
- **RTU SITES.xls**
- SCADA Division Options.ppt
- SCADA HARDWARE UPGRADE.ppt
- SCADA Sites.xls
- Scada Users Manual.zip
- **SCADA_logons.doc**
- **Security.zip**
- Standard Colors & Symbols.xls
- Station Control Testing Procedures.ppt
- **DIALUP.DOC**
- DISPLAYS.DOC
- <station> Comm Card Converter pinout.pdf
- Comm Ports for Airlink.pdf
- D-Sub to RJ45 Modular Adapters.pdf
- **SCADA Personnel.html**

Is Iran the new China?

Cyberattack on Mideast energy firms was among most destructive, Panetta says

Thierry Charlier/AFP/Getty Im
behind the so-called Shamo

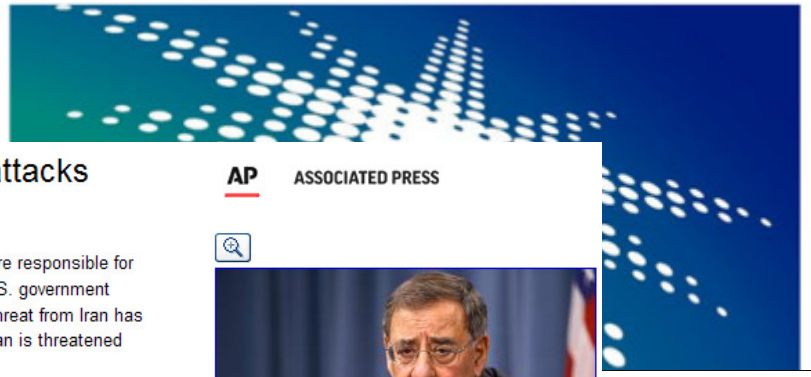
Saudi Aramco reels under curse of Shamoon virus?

By Richi Jennings
August 27, 2012 5:51 AM EDT

+ More + Briefcase

Saudi Aramco, the world's eighth largest oil refiner, is still recovering after a targeted malware attack took down 30,000 workstations. In apparent retaliation for the alleged crimes of the Saudi government, a previously-unknown hacker group claimed responsibility.

In IT Blogwatch, bloggers wonder whether this is the curse of Shamoon.



US: Hackers in Iran responsible for cyberattacks

By LOLITA C. BALDOR, Associated Press – 5 hours ago

WASHINGTON (AP) — U.S. authorities believe that Iranian-based hackers were responsible for cyberattacks that devastated Persian Gulf oil and gas companies, a former U.S. government official said. Just hours later, Defense Secretary Leon Panetta said the cyberthreat from Iran has grown, and he declared that the Pentagon is prepared to take action if American is threatened by a computer-based assault.

The former official, who is familiar with the investigation, said U.S. authorities believe the cyberattacks were likely supported by the Tehran government and came in retaliation for the latest round of American sanctions against Iran.

Before Panetta's remarks on Thursday, U.S. officials had said nothing publicly about the Gulf attacks or the investigation. But Panetta described them in a speech to business leaders in New York City, saying they were probably the most destructive cyber assault the private sector has seen to date.

Panetta did not directly link Iran to the Gulf attacks, but he said Tehran has "undertaken a concerted effort to use cyberspace to its advantage." And, he said the Pentagon has poured billions into beefing up its ability to identify the origin of a cyberattacks, block them and respond when needed.

AP ASSOCIATED PRESS

FILE - In this Sept. 27, 2012, file photo, U.S. Defense Secretary Leon Panetta, speaks at a news conference with U.S. Chairman of the Joint Chiefs of Staff Gen. Martin Dempsey, not pictured, at the Pentagon, in Washington. A former U.S. government official says American authorities firmly believe that Iranian hackers, likely supported by the Tehran government,

Shamoon Attack – Was it against ICS?

- Saudi Aramco is based in Saudi Arabia, but also maintains offices in the United States, was attacked on August 15th
- "The Cutting Sword of Justice" is claiming responsibility
- Saudi Aramco reports that approximately 30,000 machines were affected
- Saudi Aramco maintains that their oil production was not impacted as a result of this attack.

Exploitation Tools for ICS?

- The Metasploit Framework has over 50 ICS related exploits
- The GLEG Agora SCADA+ Exploit pack is a collection of exploits that specifically target industrial control system (ICS) products
- A researcher at Exodus Intelligence says he has also discovered more than 20 flaws in SCADA packages

Source: Threat Post, November 26, 2012

Did We Learn from Stuxnet?

- (**October 2012**) A US power utility contacted ICS-CERT to report a virus infection in a turbine control system which impacted approximately ten computers
- A third-party technician used an USB-drive to upload software updates during a scheduled outage for equipment upgrades
- The USB-drive was infected with the Mariposa virus. The infection resulted in downtime for the systems and delayed the plant restart by approximately three weeks

Lesson Learned:

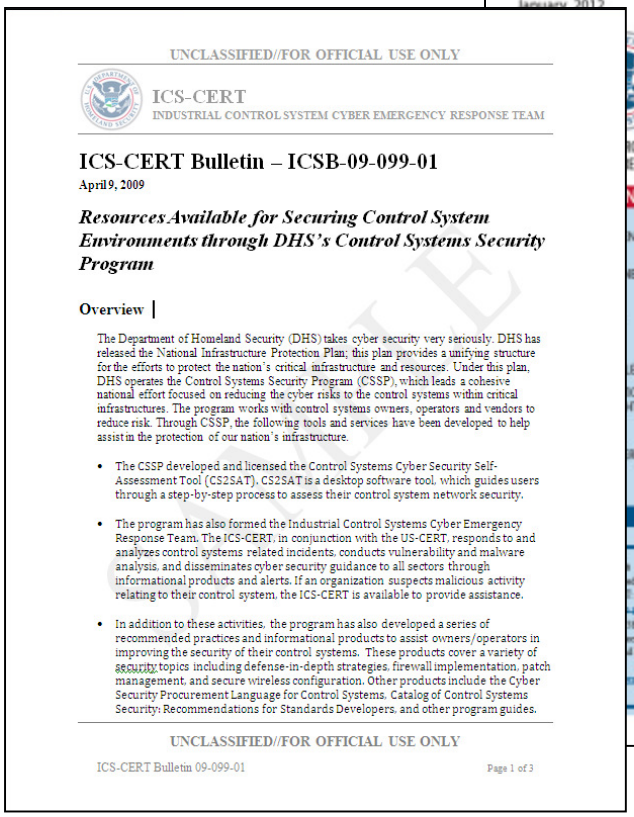
- Develop and implement baseline security policies
- Maintaining up-to-date anti-virus definitions
- Managing system patching
- Governing the use of removable media
- Managing sub-contractors

Your SCADA Devices are Attacked

- Honeypot Architectures Built
  - High-interaction
  - Low-interaction
- Events
  - 39 attacks (13 repeats)
  - Attempts to circumvent authentication to access HMI
  - Expert knowledge of Common ICS protocols
- How relevant is this data to real world

Actionable Intelligence

Alerts



UNCLASSIFIED//FOR OFFICIAL USE ONLY

ICS-CERT
INDUSTRIAL CONTROL SYSTEM CYBER EMERGENCY RESPONSE TEAM

ICS-CERT Bulletin – ICSB-09-099-01

April 9, 2009

Resources Available for Securing Control System Environments through DHS's Control Systems Security Program

Overview

The Department of Homeland Security (DHS) takes cyber security very seriously. DHS has released the National Infrastructure Protection Plan; this plan provides a unifying structure for the efforts to protect the nation's critical infrastructure and resources. Under this plan, DHS operates the Control Systems Security Program (CSSP), which leads a cohesive national effort focused on reducing the cyber risks to the control systems within critical infrastructures. The program works with control systems owners, operators and vendors to reduce risk. Through CSSP, the following tools and services have been developed to help assist in the protection of our nation's infrastructure.

- The CSSP developed and licensed the Control Systems Cyber Security Self-Assessment Tool (CS2SAT). CS2SAT is a desktop software tool, which guides users through a step-by-step process to assess their control system network security.
- The program has also formed the Industrial Control Systems Cyber Emergency Response Team. The ICS-CERT, in conjunction with the US-CERT, responds to and analyzes control systems related incidents, conducts vulnerability and malware analysis, and disseminates cyber security guidance to all sectors through informational products and alerts. If an organization suspects malicious activity relating to their control system, the ICS-CERT is available to provide assistance.
- In addition to these activities, the program has also developed a series of recommended practices and informational products to assist owners/operators in improving the security of their control systems. These products cover a variety of security topics including defense-in-depth strategies, firewall implementation, patch management, and secure wireless configuration. Other products include the Cyber Security Procurement Language for Control Systems, Catalog of Control Systems Security: Recommendations for Standards Developers, and other program guides.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

ICS-CERT Bulletin 09-099-01 Page 1 of 3

Reports

ICS-CERT MONTHLY MONITOR

January 2012

NOTEWORTHY INCIDENTS IN DECEMBER

Chemical Sector

Recently, ICS-CERT responded to a reported cyber incident at a US chemical company. The company reported the presence of an infection in their business network and they suspected that data had been exfiltrated. In response to the initial report, ICS-CERT provided extensive analytical support to the company, including analysis of file system images, memory dumps, firewall logs, and malware samples.

At the request of the company, ICS-CERT deployed an on-site fly away team to work directly with company personnel to conduct further analysis and gather additional data to further the investigation of the incident. ICS-CERT analysis confirmed the presence advance persistent malware and sophisticated techniques to maintain presence. Interestingly, the malware did not appear to propagate opportunistically like traditional malware, an indication that it was possibly more directed in choosing its victim hosts.

ICS-CERT assisted the company with identifying the scope of the infection and by providing analysis and mitigations for eradicating the threat actor from their network. Asset owners and operators should consider the value of their Intellectual Property (IP) and use defense in depth strategies to protect their networks and data.

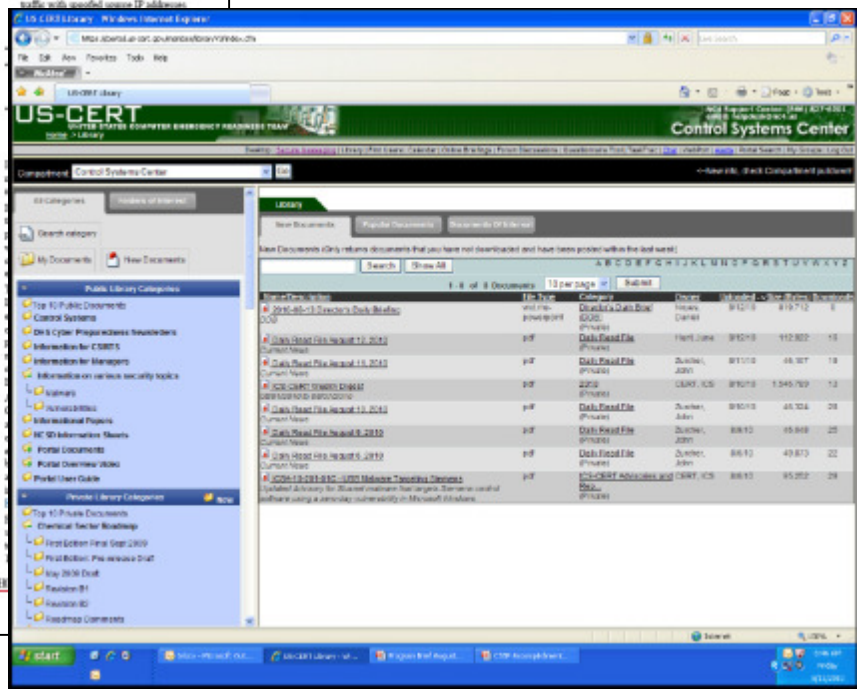
Transportation Sector

In early December, 2011, ICS-CERT responded to a cybersecurity incident affecting a rail company. The initial report indicated that the rail company was experiencing a cyber attack to its secondary communications equipment.

ICS-CERT, working in coordination with US-CERT and the asset owner, analyzed various data and determined that the incident was not the result of a targeted attack. In this case, the rail company quickly implemented effective measures to maintain the safety of its operation and worked closely with ICS-CERT to understand the incident and take appropriate

Partner Collaboration

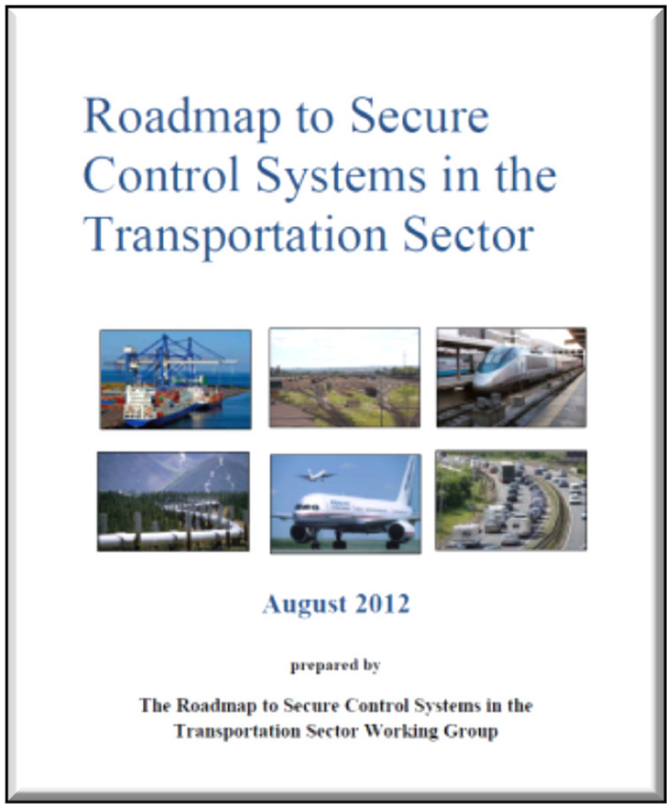
Web site & Portal



ICS Cybersecurity Training

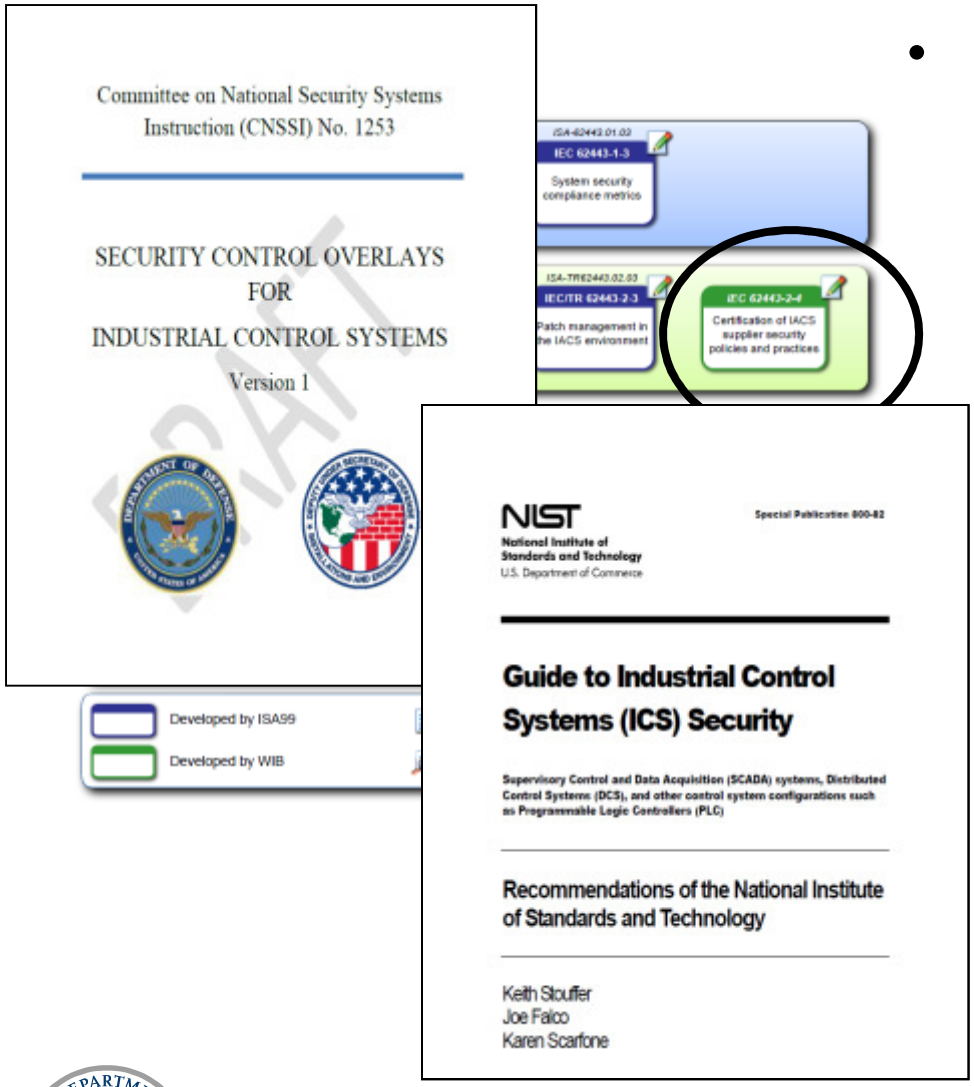
*IOSS first place award 2008

ICS – Joint Working Group



- Provides a vehicle for collaboration between government and private sector control systems stakeholders
  - Government Coordinating Council
  - Sector Coordinating Council
  - Subject Matter Experts
  - International Community
- Fosters information sharing and coordination of activities and programs across government and private industry stakeholders involved in protecting CIKR
- Includes 6 subgroups
  - Vendors
  - International
  - Workforce Develop
  - Research and Development
  - ICS Roadmap Development
  - **Standards**

ICS Standards Efforts



- CNSSI 1253 ICS Overlay
  - Pentagon March Memo for base commanders to perform assessments on all ICS

ISO/IEC 62443 Series

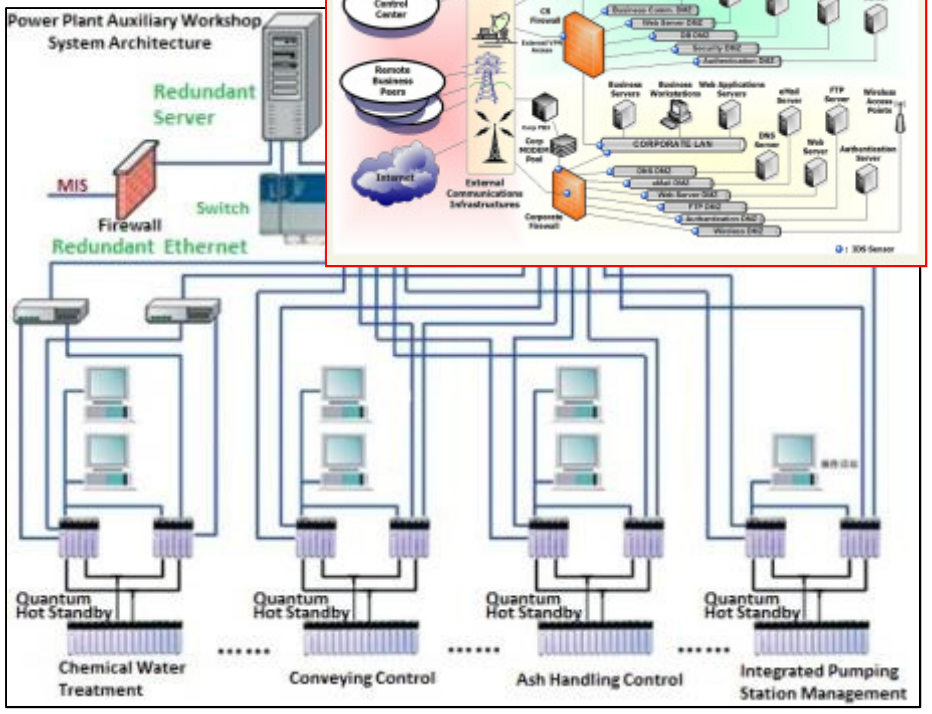
- Security for ICS suppliers, owners, and integrators
- Uses ISA-99 & WIB as basis

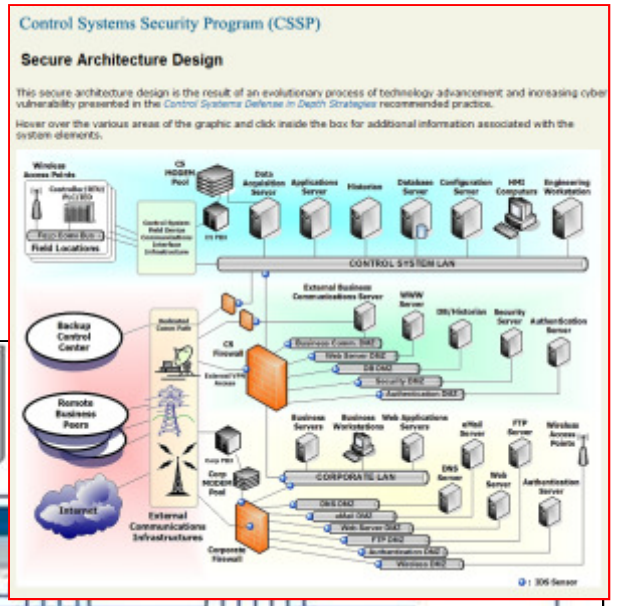
NIST SP 800-82 Overlay

- Overlay to SP 800-53 Rev.4 controls
- Pre-Draft to ICSJWG Standards Group for review/comment
- Public Draft on September 30th

Control System SME Assessments

- Assessment using CSET (1-day)
  - Over-the-shoulder
- Design Architecture Review
  - 2-3 Days to complete
  - Robust architecture analysis
  - Network design review
- Network Architecture Verification and Validation
  - Includes discovery process
  - Study of interdependencies
  - Ideal for High-security ICS





Cyber Security Evaluation Tool (CSET)

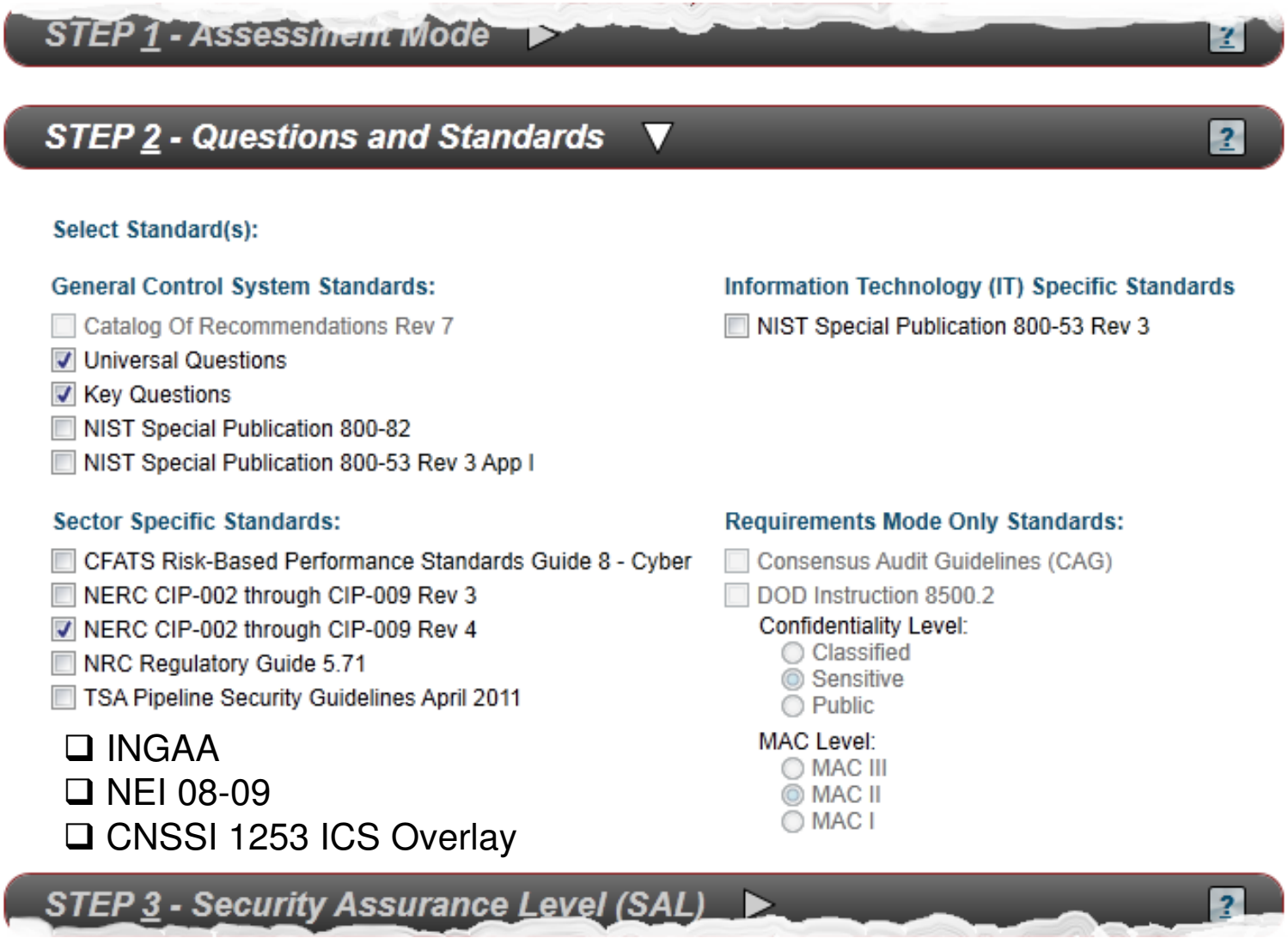
- Stand-alone Software application
- Self-assessment using recognized standards
- Tool for integrating cybersecurity into existing corporate risk management strategy

CSET Download:

www.ics-cert.us-cert.gov/Downloading-and-Installing-CSET

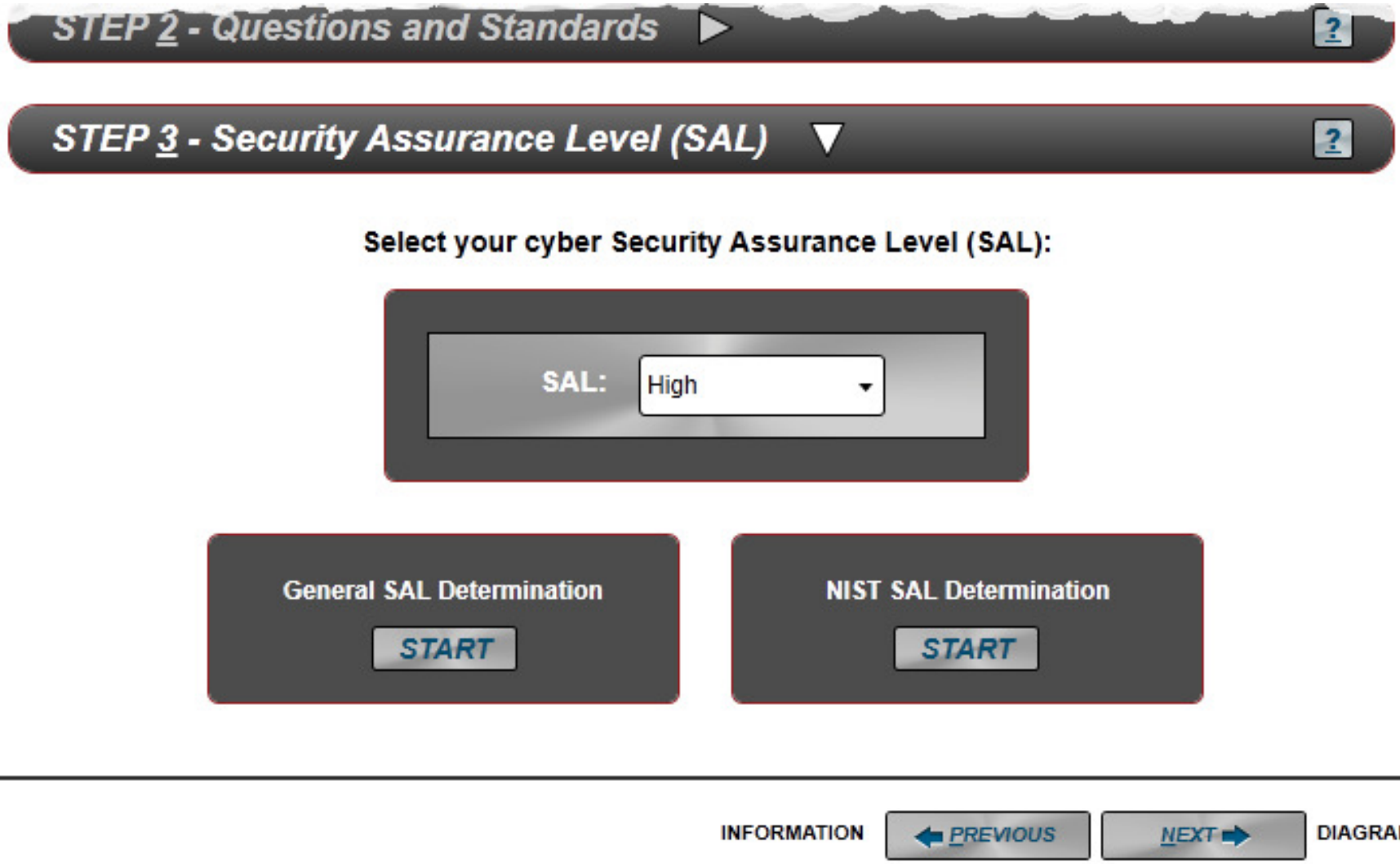
Homeland Security

Questions & Standards

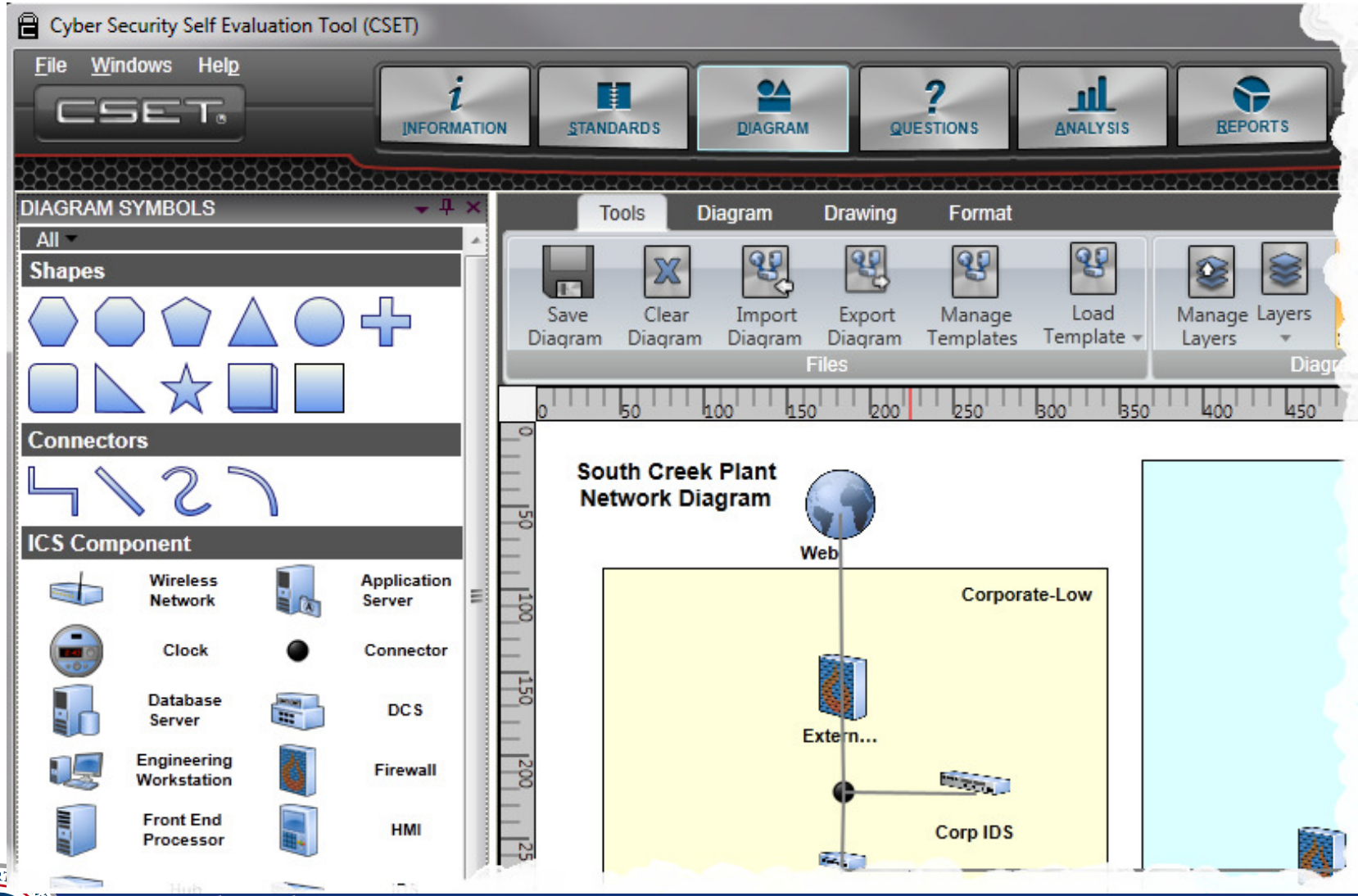


- ❑ INGAA
- ❑ NEI 08-09
- ❑ CNSSI 1253 ICS Overlay

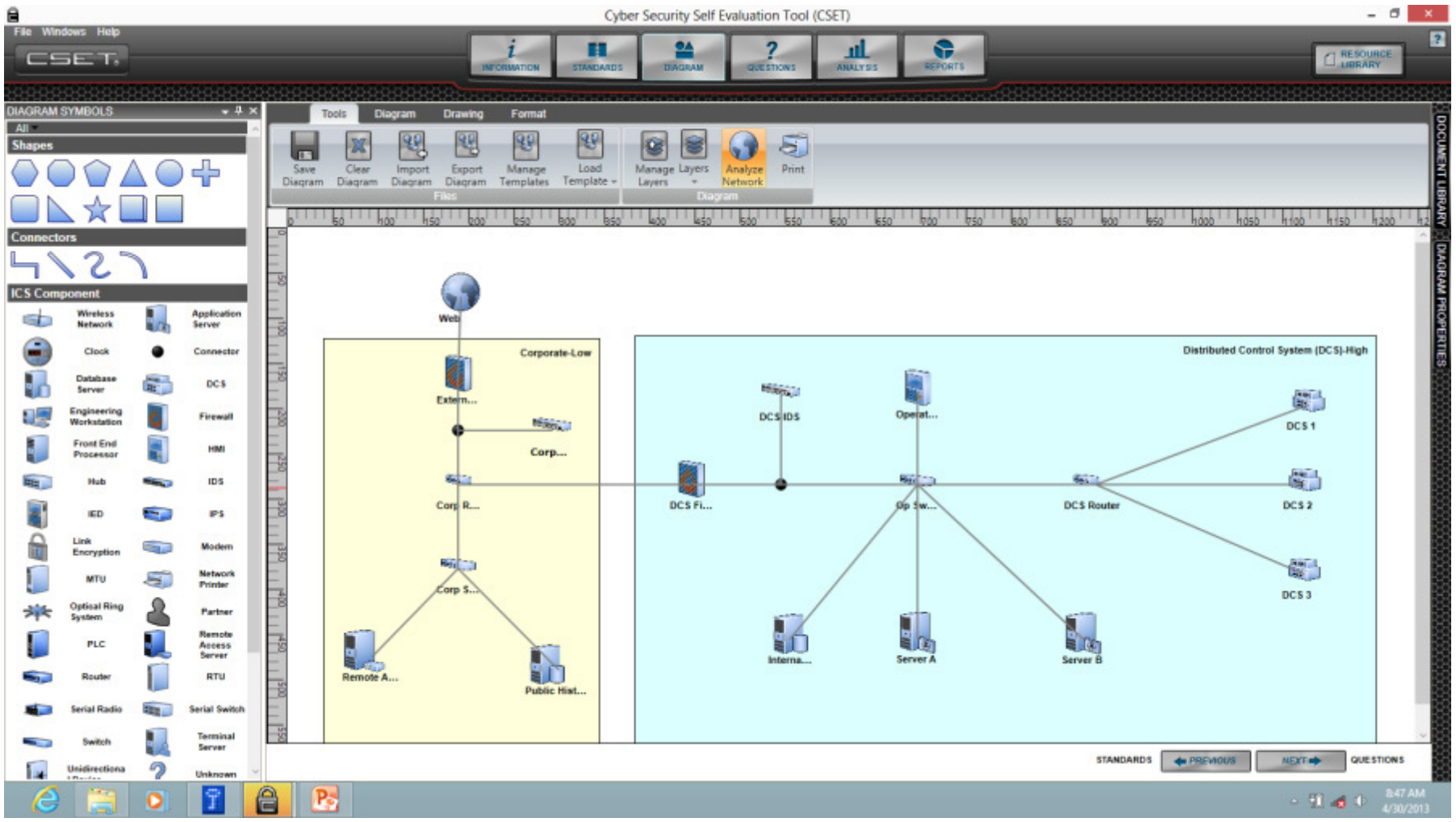
Security Assurance Level (SAL)



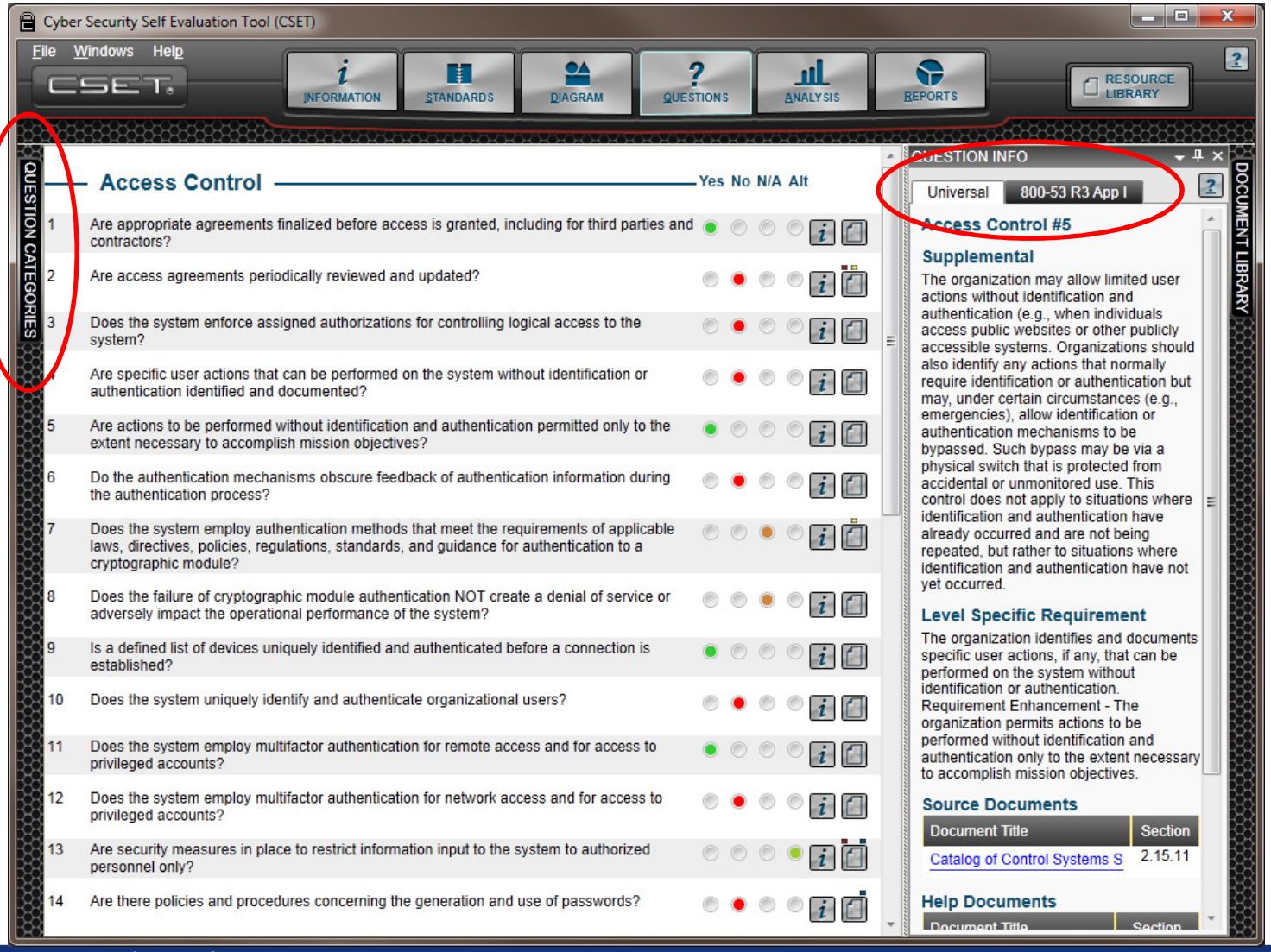
Diagramming Tool



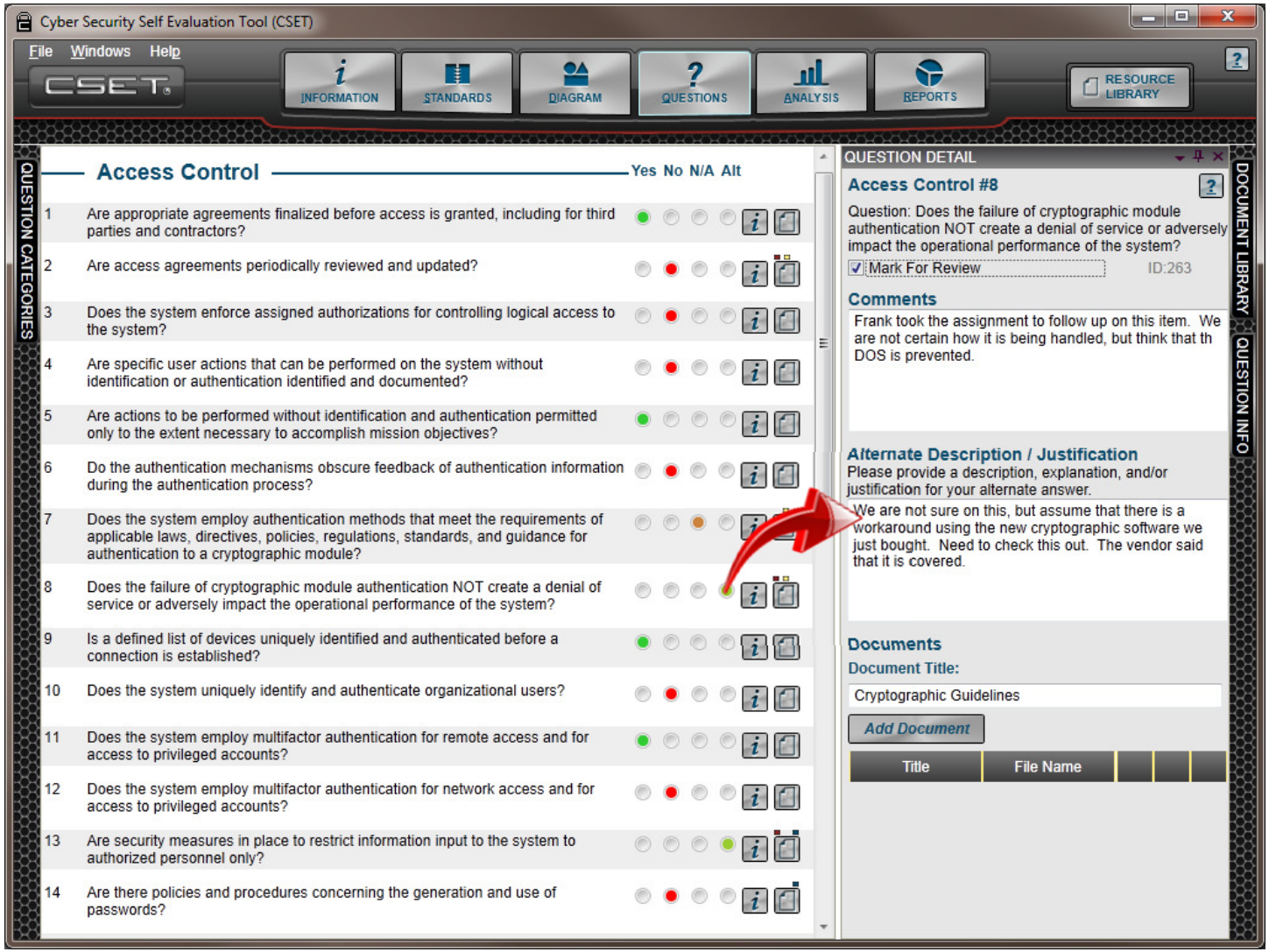
Component Diagram Tool



Question Information



Comments, Marked and Alternates



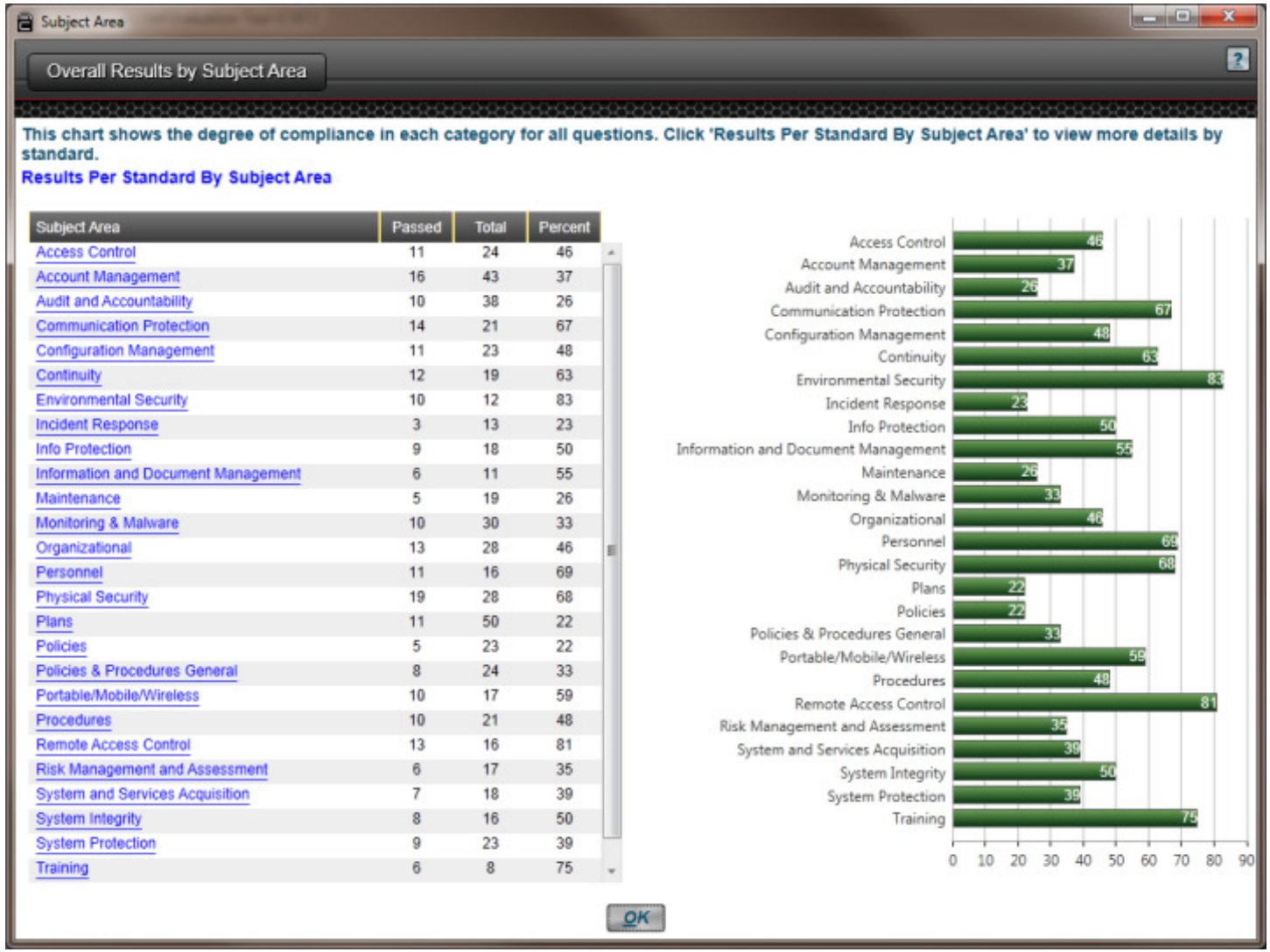
Dashboard Analysis

Analysis Detail Screens

	Yes	NA	Alt	Total	Percent
Boundary Protection	3	0	0	9	33
Firewall	7	0	0	17	41
Host Intrusion Detection	0	0	0	3	0
Intrusion Detection	0	0	3	3	100
Logging	4	0	0	20	20
Management	4	0	0	4	100

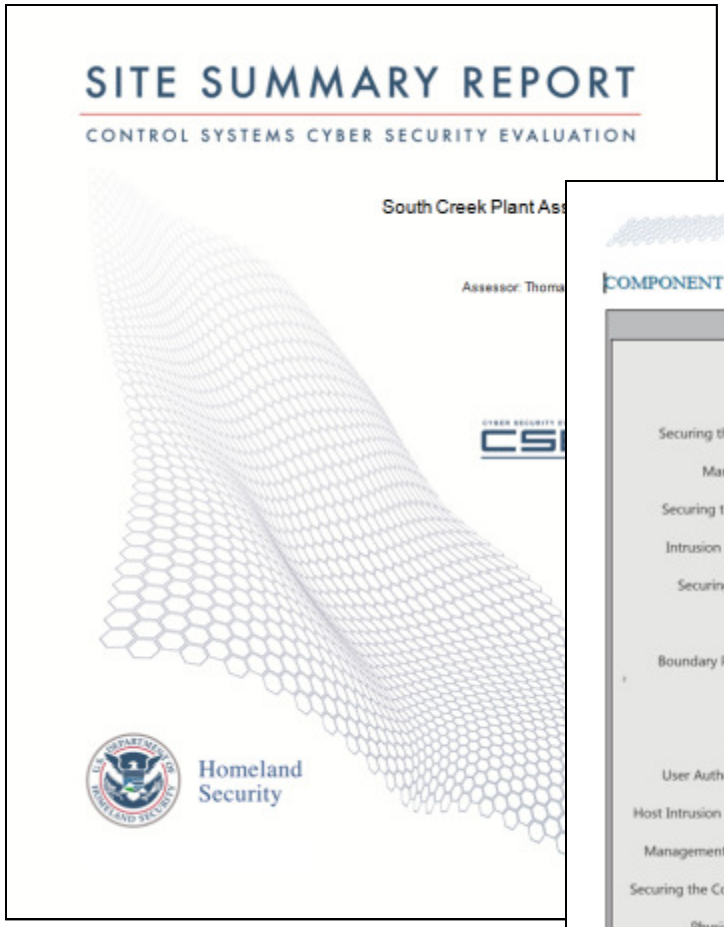
Component	# Components	Total	Yes	No	N/A
Application Server	2	2	2	0	0
Database Server	3	80	24	56	0
Engineering Workstation	3	3	0	3	0
Firewall	5	19	13	6	0
Front End Processor	2	59	22	35	0
HMI	4	2	0	2	0

Analysis Detail - Example



Subject Area	Passed	Total	Percent
Access Control	11	24	46
Account Management	16	43	37
Audit and Accountability	10	38	26
Communication Protection	14	21	67
Configuration Management	11	23	48
Continuity	12	19	63
Environmental Security	10	12	83
Incident Response	3	13	23
Info Protection	9	18	50
Information and Document Management	6	11	55
Maintenance	5	19	26
Monitoring & Malware	10	30	33
Organizational	13	28	46
Personnel	11	16	69
Physical Security	19	28	68
Plans	11	50	22
Policies	5	23	22
Policies & Procedures General	8	24	33
Portable/Mobile/Wireless	10	17	59
Procedures	10	21	48
Remote Access Control	13	16	81
Risk Management and Assessment	6	17	35
System and Services Acquisition	7	18	39
System Integrity	8	16	50
System Protection	9	23	39
Training	6	8	75

Hardcopy Reports with Recommendations

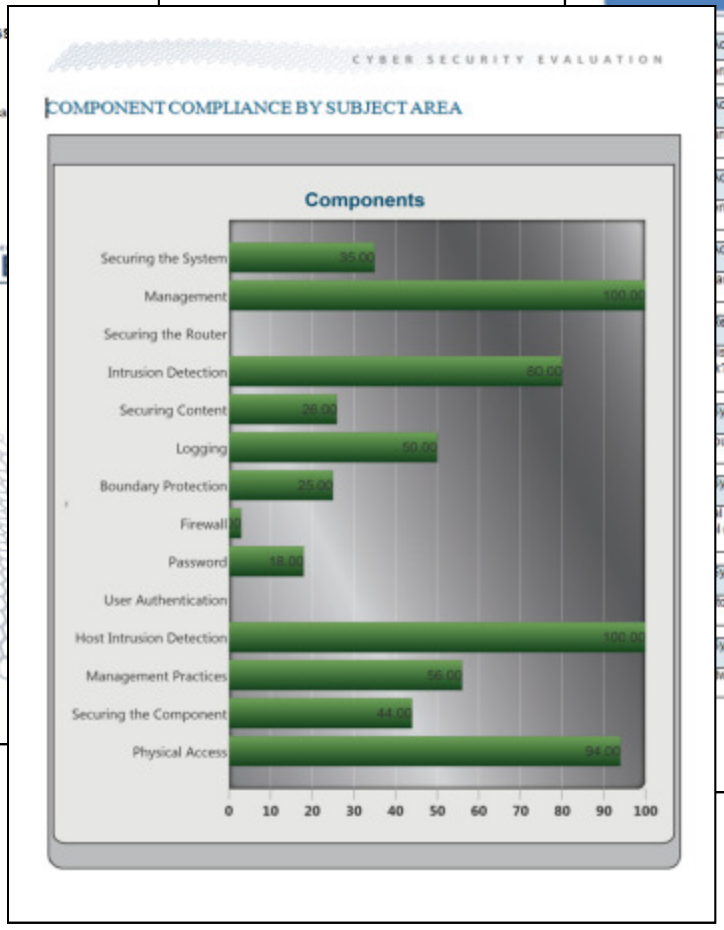

SITE SUMMARY REPORT

CONTROL SYSTEMS CYBER SECURITY EVALUATION

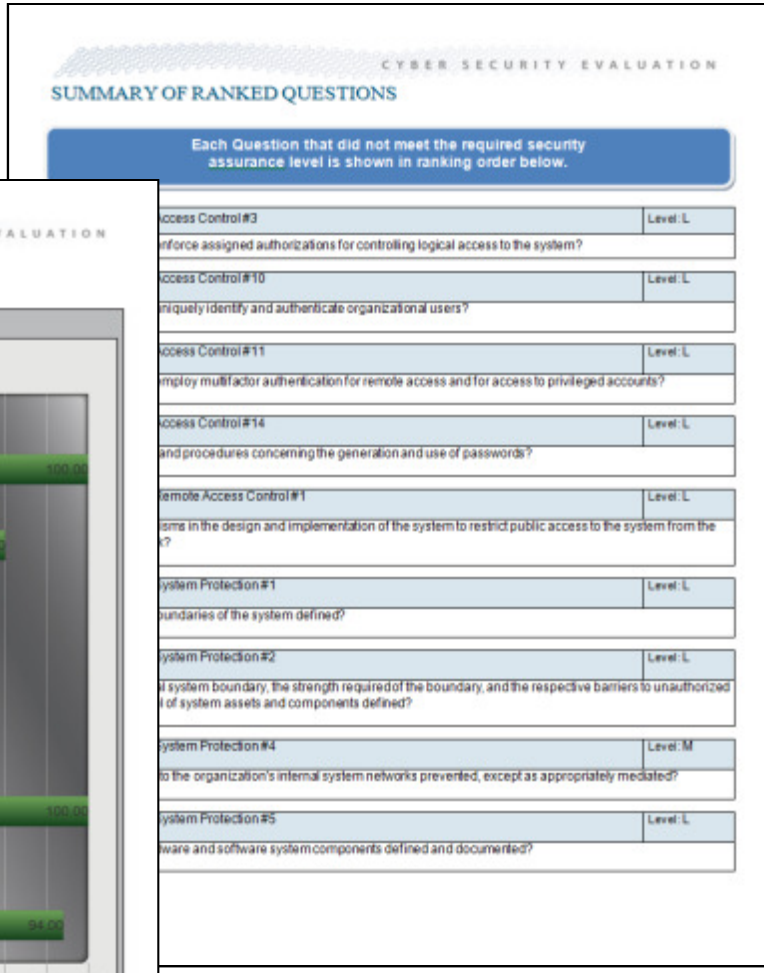
South Creek Plant As

Assessor: Thoma

Homeland Security


CYBER SECURITY EVALUATION

COMPONENT COMPLIANCE BY SUBJECT AREA

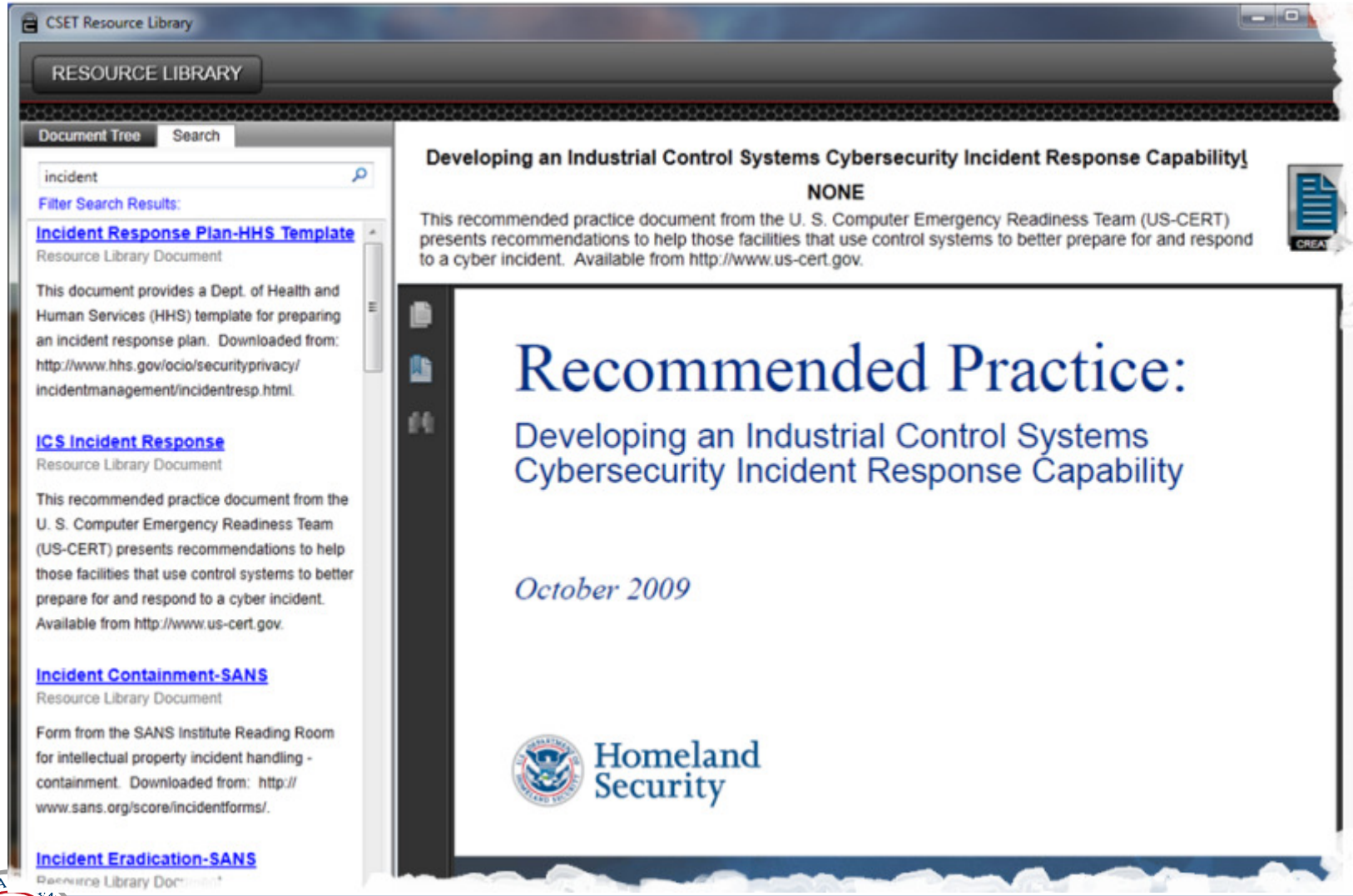

CYBER SECURITY EVALUATION

SUMMARY OF RANKED QUESTIONS

Each Question that did not meet the required security assurance level is shown in ranking order below.

ccess Control #3	Level: L
nforce assigned authorizations for controlling logical access to the system?	
ccess Control #10	Level: L
niquely identify and authenticate organizational users?	
ccess Control #11	Level: L
mploy multifactor authentication for remote access and for access to privileged accounts?	
ccess Control #14	Level: L
nd procedures concerning the generation and use of passwords?	
emote Access Control #1	Level: L
sms in the design and implementation of the system to restrict public access to the system from the	
ystem Protection #1	Level: L
undaries of the system defined?	
ystem Protection #2	Level: L
l system boundary, the strength required of the boundary, and the respective barriers to unauthorized l of system assets and components defined?	
ystem Protection #4	Level: M
o the organization's internal system networks prevented, except as appropriately mediated?	
ystem Protection #5	Level: L
ware and software system components defined and documented?	

Resource Library - Search



CSET 6.0 Enhancements

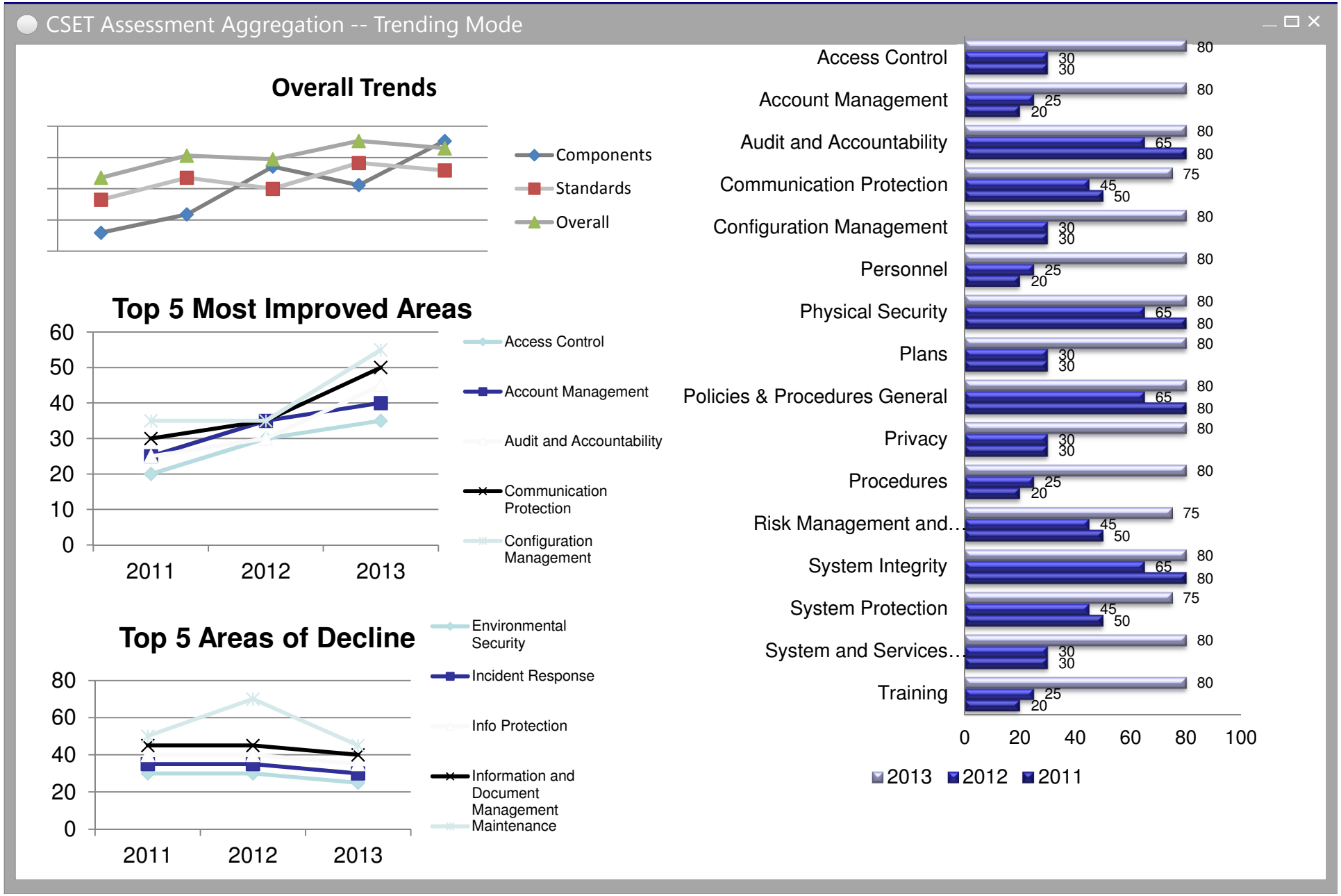
New/Updated Standards

- NEI 08-09 Rev 6
- NISTIR 7628 Ver 1 (August 2010)
- INGAA Ver 1 (January 31, 2011)
- NIST SP800-53 Appendix J Rev 4
- NIST SP800-82 Rev 1 (May 2013)
- CNSSI ICS Overlay Update

New Evaluation Capabilities

- Merging
- Comparison
- Aggregation
- Trending

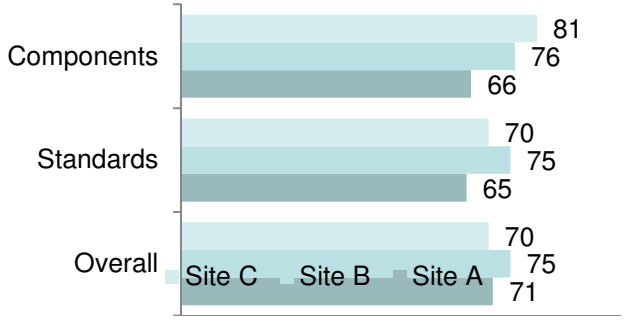
Trending Sample Screen

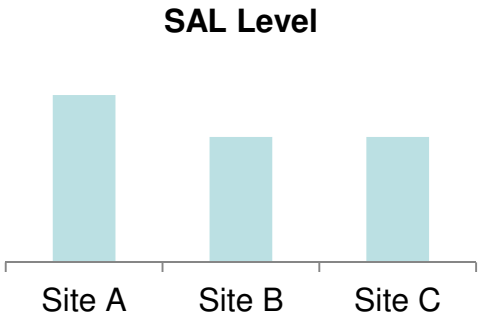


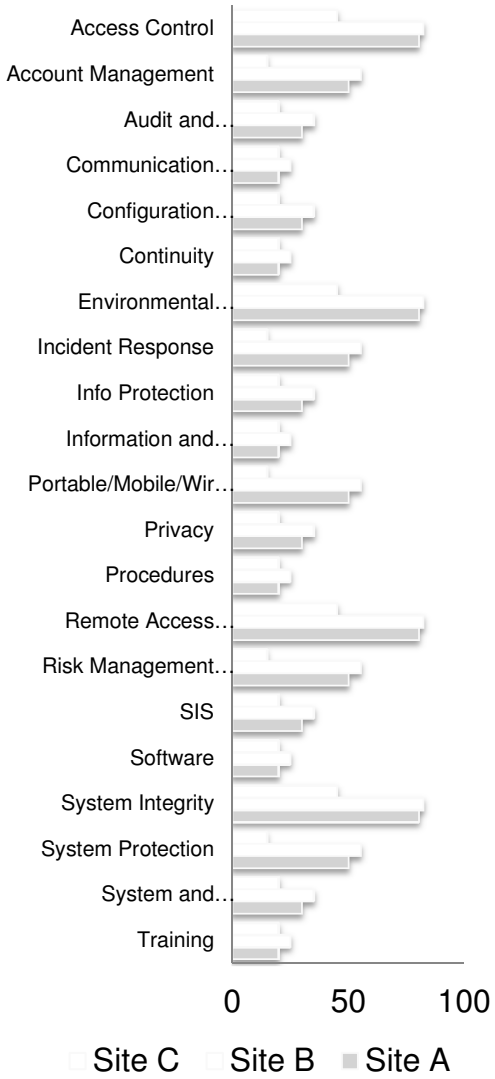
Aggregation Sample Screen

CSET Assessment Aggregation – Comparison Mode

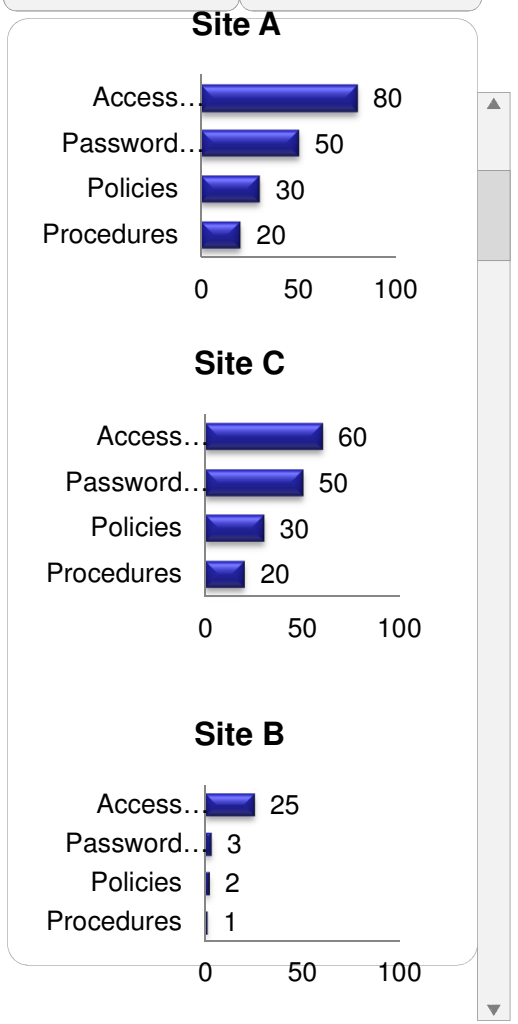
Site	Total Questions Answered	Yes	No
Site A	560	300	260
Site B	342	300	42
Site C	268	152	116







Sort By Best | Sort By Worst

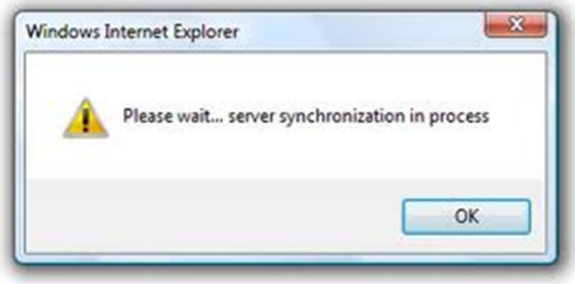


CSET 6.0 Enhancements (cont.)

New/Updated Functionality

- Inventory Lists
- Security Plans
- YouTube Tutorials
- Updated Diagramming Tool

What if Boom?


Windows Internet Explorer
Please wait... server synchronization in process
OK


Not
Funny


PLEASE
HACK MY
COMPUTER!


SYSTEM FAILURE


VIRUS:

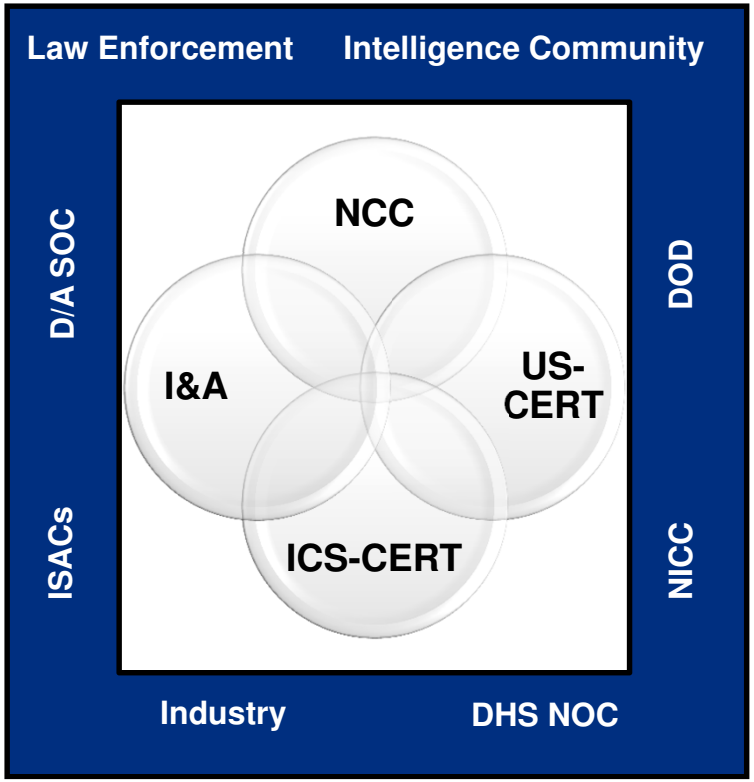
National Cybersecurity Team

Each Department has distinct, yet complementary roles:

- **DHS:** responsible for coordinating the domestic all-hazards preparedness efforts of executive departments and agencies
- **DOJ:** responsible for responding to domestic counterterrorism, intelligence, and law enforcement activities
- **DOD:** responsible for national defense, foreign cyber intelligence, protection of national security systems

NCCIC Partnerships

- NCCIC is comprised of organizational components and operational liaisons
  - *Components refers to DHS organizations that have a major presence on the NCCIC floor*
  - *Operational Liaisons refer to outside agencies such as ISACs, Law Enforcement and Industry*
- The execution of NCCIC's mission relies on coordinated operations that contribute to all products and services



NCCIC Components

Incident Reporting

NCCIC 24 X 7 Watch and Warning (W&W) provides real-time threat analysis and incident reporting capabilities

- W&W contact number: 1-888-282-0870

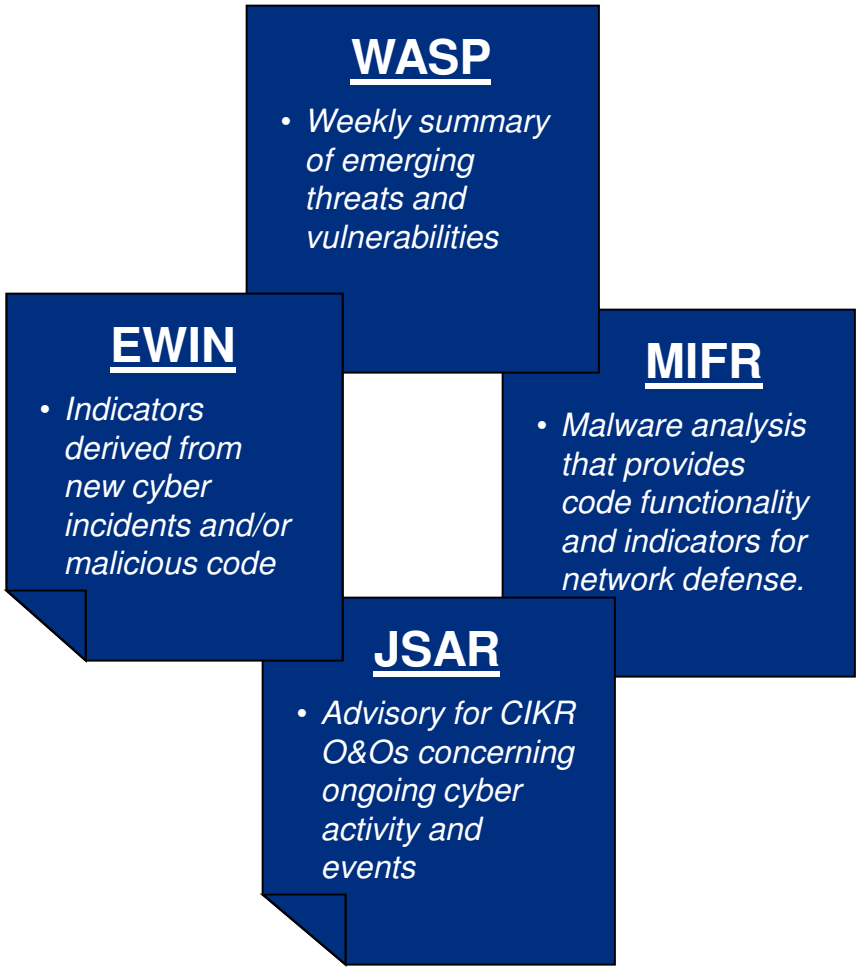
Malware Submission Process:

- Please send all submissions to AMAC at: submit@malware.us-cert.gov
- Must be provided in password-protected zip files using password “infected”
- Alternate Method: Web-submission page created for use when email submission is not possible: https://malware.us-cert.gov

NCCIC Resources

- US-CERT/ICS-CERT Portal Example Products
  - Early Warning and Indicator Notice (EWIN)
  - Weekly Analytic Synopsis Product (WASP)
  - Joint Security Awareness Report (JSAR)
  - Malware Initial Findings Report (MIFR)
- Homeland Security Information Network – Critical Sectors (HSIN-CS)
- Exercises
  - Cyber Storm
  - National Level-Exercises
- Assessments

NCCIC Products



Protecting Your Information

Traffic-Light Protocol (TLP): Originator-controlled classification system developed to encourage greater sharing of sensitive (but unclassified) information with external entities.

When should it be used?	TLP Color	How may it be shared?
Sources may use TLP: RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	RED	Recipients may not share TLP: RED information with any parties outside of the specific exchange, meeting or conversation in which it is originally disclosed.
Sources may use TLP: AMBER when information requires support to be effectively acted upon, but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	AMBER	Recipients may only share TLP: AMBER information with members of their own organization, and only as widely as necessary to act on that information.
Sources may use TLP: GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	GREEN	Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels.
Sources may use TLP: WHITE when information carries minimal or no risk of misuse, in accordance with applicable rules and procedures for public release.	WHITE	TLP: WHITE information may be distributed without restriction, subject to copyright controls.

What should I do?

- If you are the “boss” – engineering manager, operations manager etc. – Make sure your staff have cybersecurity training and the tools and resources needed to “do the job”
- If you are technical staff – control systems engineer, security specialist, systems administrator – make sure your “boss” knows the risks where you have systems with weak security
- Know your system(s)! Most network diagrams are outdated and not very useful during a breach – update them!
- Check the ICS-CERT website – sign up for alerts and advisories, and use the recommended practices we post

In Closing

- Security around ICS systems could certainly use improvement in all sectors (water, energy – ONG & electricity, nuclear, etc.)
- Don’t hook your ICS system to the internet
- When you think you have a breach, reach out to the experts
- Scanning activity should be considered normal for internet facing devices
- Log everything and review your logs regularly for anomolies!

Homeland Security

Cybersecurity is a shared responsibility

Lisa Kaiser, Lisa.Kaiser@dhs.gov

Learn more about the DHS Control Systems Security Program

www.ics-cert.us-cert.gov cssp@dhs.gov

Download CSET

http://ics-cert.us-cert.gov/Downloading-and-Installing-CSET

Report Control Systems cyber incidents & vulnerabilities and sign up for alerts and advisories

ICS-CERT@dhs.gov

Toll Free: 1-877-776-7585 International: 1-208-526-0900

Homeland Security