

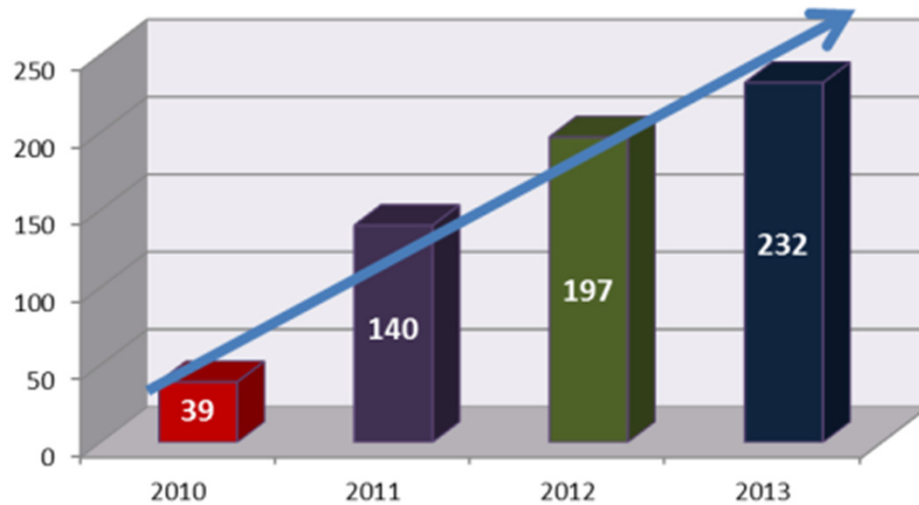


NIBS Cybersecurity Overview

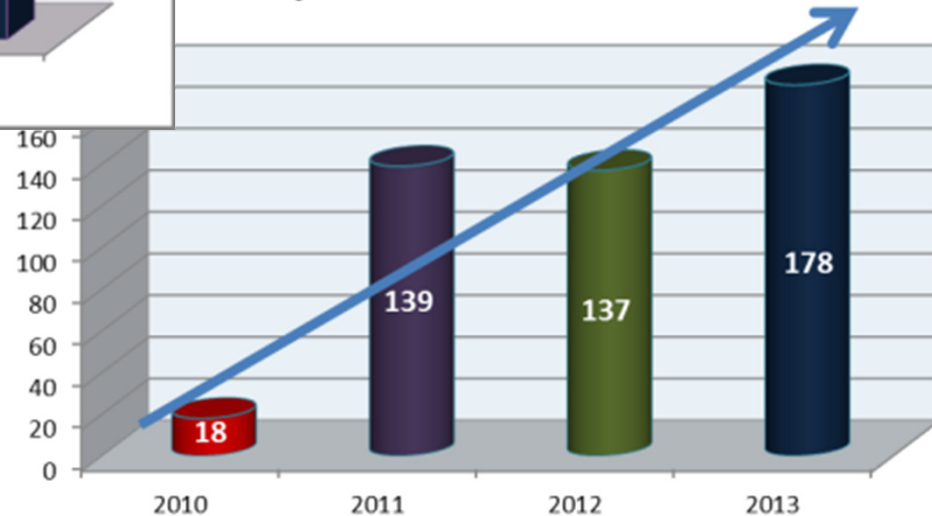
**Lisa Kaiser – Standards Chief
Control Systems Security / ICS-CERT**

ICS-CERT Metrics

Reported Incidents



Reported Vulnerabilities



Homeland
Security

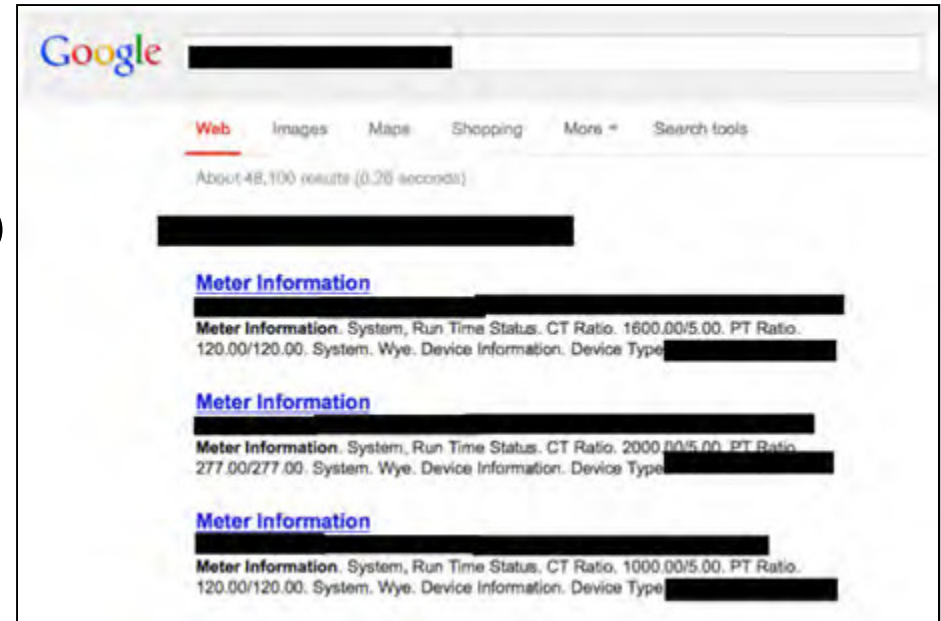
New Threat - Cyber Researchers

- 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



Router**Passwords**.com

default password list



Homeland
Security

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

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.

Saudi Aramco reels under curse of Shamoon virus?

By Richi Jennings

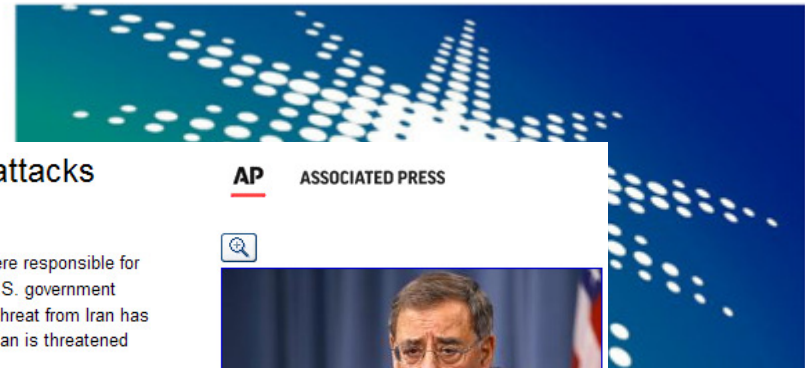
August 27, 2012 5:51 AM EDT

[+ 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.



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,



Homeland
Security

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



Homeland
Security

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



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 infrastructure. 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

ICS-CERT MONTHLY MONITOR

January 2012



CONTROL SYSTEMS
RESPONSE TEAM

NOTES

NTS

MESS

LEAVES

IGNAL

NTS

ABILITY

ed to this report

Security Program

Incident

ICS-CERT

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 the system images, memory dumps, firewall logs, and malware samples.

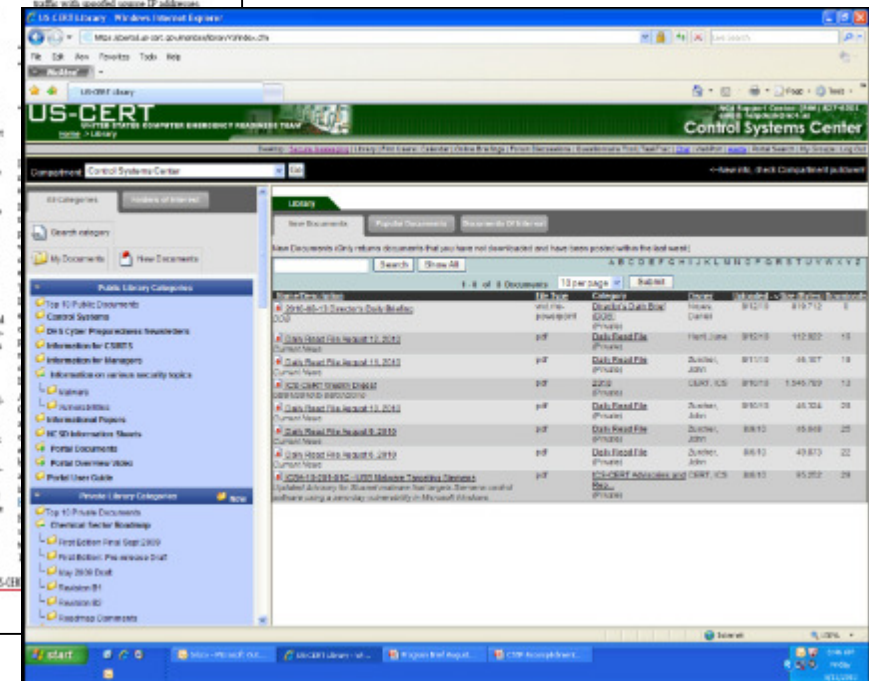
At the request of the company, ICS-CERT deployed an on-site fly away team to work directly with company personnel to conduct further analysis and gather additional data to further the investigation of the incident. ICS-CERT analysis confirmed the presence of a persistent malware and sophisticated techniques to maintain presence. Interestingly, the malware did not appear to propagate exponentially 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 mitigation 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 operations and worked closely with ICS-CERT to understand the incident and take appropriate

mitigating measures. ICS-CERT made the following determinations:

- Redundant communications equipment at the web layer received erroneous DNS traffic with spoofed source IP addresses.



Partner Collaboration

Reports Web site & Portal



Homeland
Security

ICS Cybersecurity Training

The screenshot displays the ICS-CERT website in a web browser. The browser's address bar shows the URL <http://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT>. The website header includes the ICS-CERT logo and the text "INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM". A navigation menu at the top lists: HOME, ABOUT, ICS/JWG, INFORMATION PRODUCTS, TRAINING, FAQ, and LEGAL. On the left side, a sidebar menu under "Control Systems" lists: Home, Calendar, ICS/JWG, Information Products, Training, Recommended Practices, Assessments, Standards & References, Related Sites, and FAQ. The main content area is titled "Training Available Through ICS-CERT" and contains the following text:

Scheduled training is on the ICS-CERT Calendar.

Web-Based Training
OPSEC for Control Systems

Instructor Led Format—Introductory Level
Introduction to Control Systems Cybersecurity (101)—1 day or 8 hrs

Instructor Led Format—Intermediate Level
Intermediate Cybersecurity for Industrial Control Systems (201), lecture only—1 day or 8 hrs

Hands-On Format—Intermediate Level
Intermediate Cybersecurity for Industrial Control Systems (202), with lab/exercises—1 day or 8 hrs

Hands-On Format—Technical Level
ICS Cybersecurity (301)—5 days

The ICS-CERT program provides training courses and workshops at venues associated with regional events. Refer to the ICS-CERT calendar for a schedule of these training options.

Instructor Led Format—Introductory Level

Introduction to Control Systems Cybersecurity (101)

The purpose of this course is to introduce students to the basics of industrial control systems security. This includes a comparative analysis of IT and control system architecture, security vulnerabilities, and mitigation strategies unique to the control system domain.

This course is split into four sessions: (1) Cybersecurity Landscape: Understanding the Risks, (2) Industrial Control Systems Applications, (3) Current State of Cybersecurity in Industrial Control Systems, and (4) Practical Applications of Cybersecurity.

This course is presented at regional venues in various locations throughout the year. Refer to the ICS-CERT calendar for a schedule of this training option. It will also be available as a Web-Based training course in early 2014.

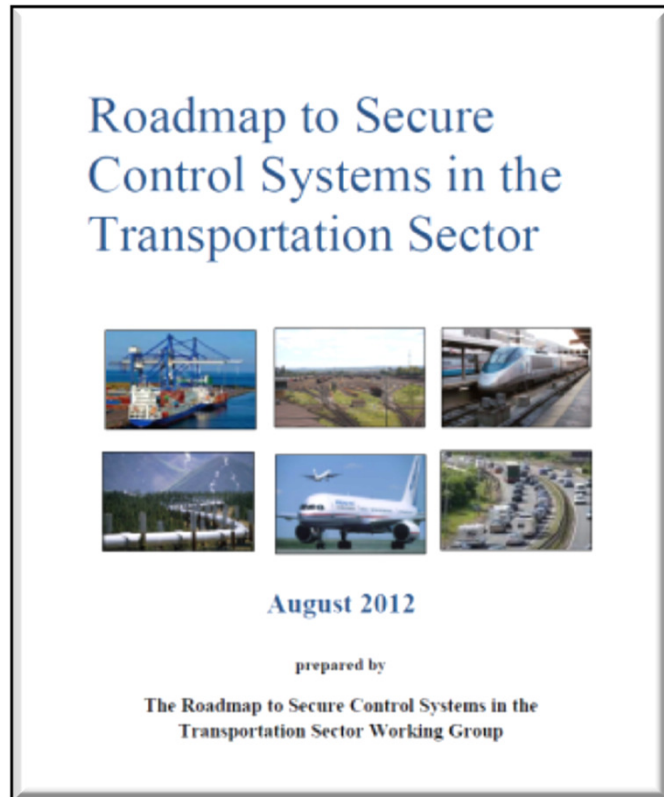
Back to top

*IOSS first place award 2008



Homeland
Security

ICS – Joint Working Group

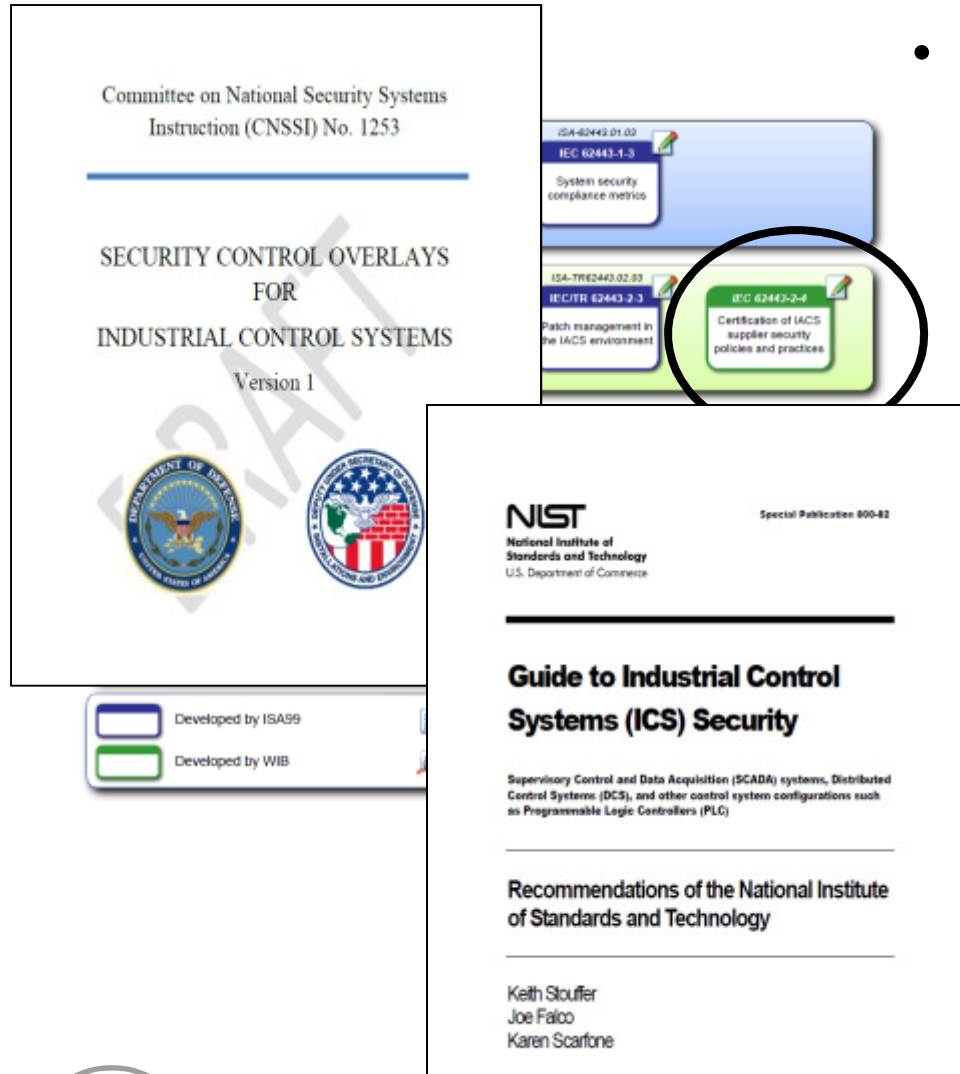


- Provides a vehicle for collaboration between government and private sector control systems stakeholders
 - Government Coordinating Council
 - Sector Coordinating Council
 - Subject Matter Experts
 - International Community
- Fosters information sharing and coordination of activities and programs across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



Homeland
Security

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



Homeland
Security

-



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

STEP 1 - Assessment Mode ▶



STEP 2 - Questions and Standards ▼



Select Standard(s):

General Control System Standards:

- ☐ Catalog Of Recommendations Rev 7
- ☒ Universal Questions
- ☒ Key Questions
- ☐ NIST Special Publication 800-82
- ☐ NIST Special Publication 800-53 Rev 3 App I

Sector Specific Standards:

- ☐ CFATS Risk-Based Performance Standards Guide 8 - Cyber
- ☐ NERC CIP-002 through CIP-009 Rev 3
- ☒ NERC CIP-002 through CIP-009 Rev 4
- ☐ NRC Regulatory Guide 5.71
- ☐ TSA Pipeline Security Guidelines April 2011
- ☐ INGAA
- ☐ NEI 08-09
- ☐ CNSSI 1253 ICS Overlay

Information Technology (IT) Specific Standards

- ☐ NIST Special Publication 800-53 Rev 3

Requirements Mode Only Standards:

- ☐ Consensus Audit Guidelines (CAG)
- ☐ DOD Instruction 8500.2

Confidentiality Level:

- ☐ Classified
- ☒ Sensitive
- ☐ Public

MAC Level:

- ☐ MAC III
- ☒ MAC II
- ☐ MAC I

STEP 3 - Security Assurance Level (SAL) ▶



Homeland
Security

Security Assurance Level (SAL)

STEP 2 - Questions and Standards

STEP 3 - Security Assurance Level (SAL)

Select your cyber Security Assurance Level (SAL):

SAL: High

General SAL Determination

START

NIST SAL Determination

START

INFORMATION

← PREVIOUS

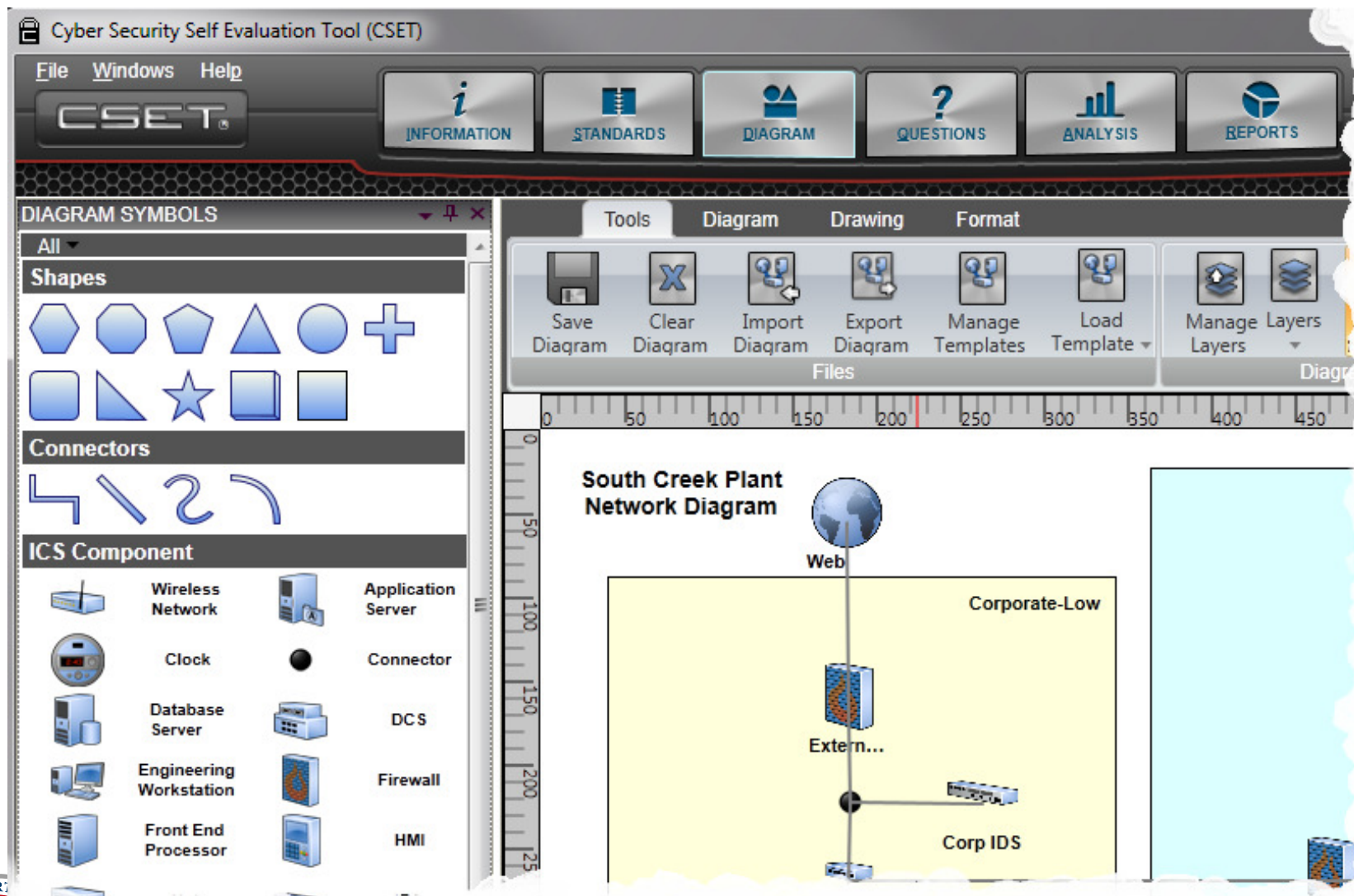
NEXT →

DIAGRAM



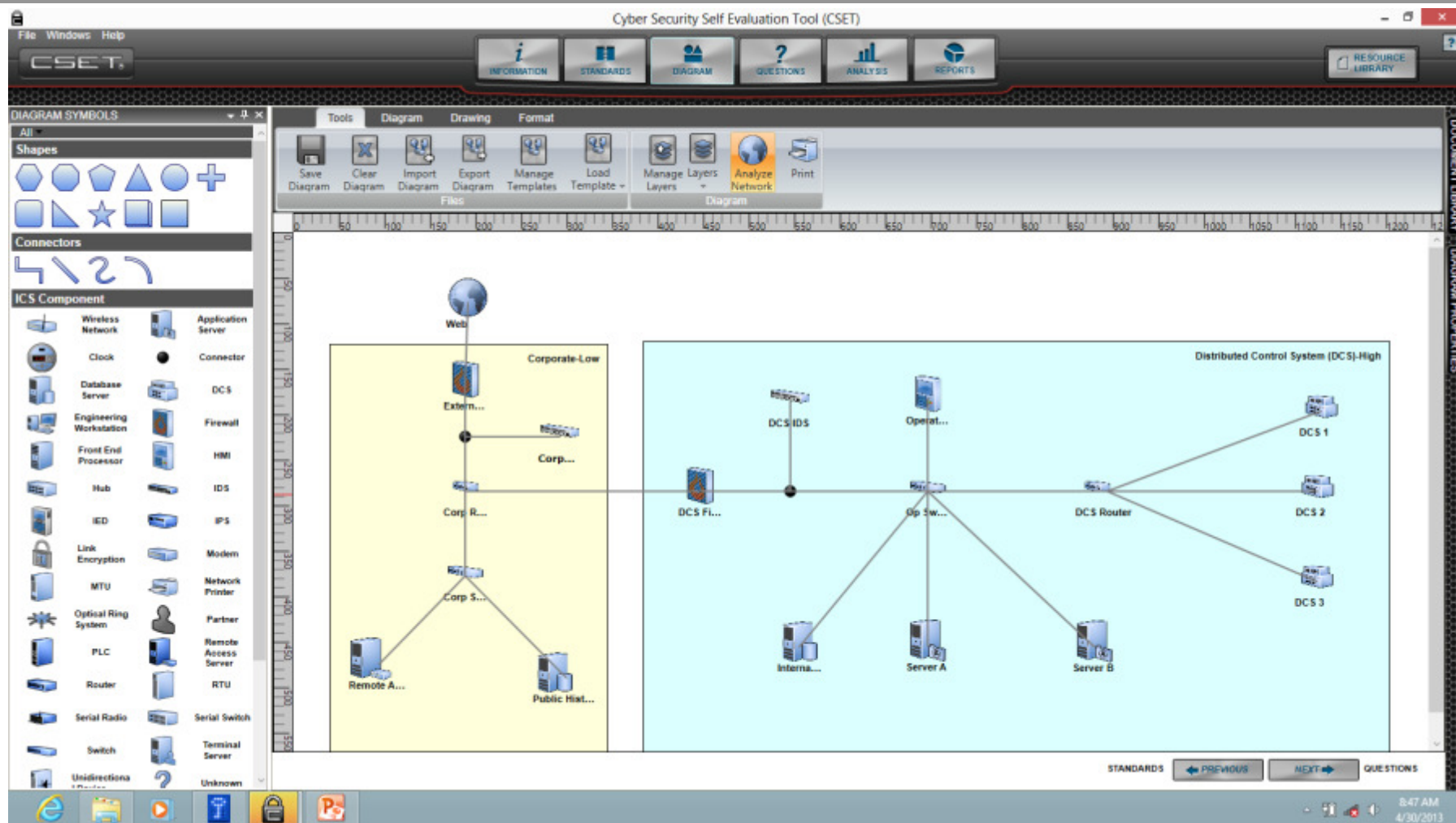
Homeland
Security

Diagramming Tool




Homeland
Security

Component Diagram Tool



Homeland
Security


 U.S. Department of Homeland Security
 24

Comments, Marked and Alternates

Cyber Security Self Evaluation Tool (CSET)

File Windows Help

CSET

INFORMATION STANDARDS DIAGRAM QUESTIONS ANALYSIS REPORTS RESOURCE LIBRARY

Access Control Yes No N/A Alt

QUESTION CATEGORIES	QUESTION	Yes	No	N/A	Alt	Info	Mark
1	Are appropriate agreements finalized before access is granted, including for third parties and contractors?	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>		
2	Are access agreements periodically reviewed and updated?	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>		
3	Does the system enforce assigned authorizations for controlling logical access to the system?	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>		
4	Are specific user actions that can be performed on the system without identification or authentication identified and documented?	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>		
5	Are actions to be performed without identification and authentication permitted only to the extent necessary to accomplish mission objectives?	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>		
6	Do the authentication mechanisms obscure feedback of authentication information during the authentication process?	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>		
7	Does the system employ authentication methods that meet the requirements of applicable laws, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module?	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>		
8	Does the failure of cryptographic module authentication NOT create a denial of service or adversely impact the operational performance of the system?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>		
9	Is a defined list of devices uniquely identified and authenticated before a connection is established?	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>		
10	Does the system uniquely identify and authenticate organizational users?	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>		
11	Does the system employ multifactor authentication for remote access and for access to privileged accounts?	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>		
12	Does the system employ multifactor authentication for network access and for access to privileged accounts?	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>		
13	Are security measures in place to restrict information input to the system to authorized personnel only?	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>		
14	Are there policies and procedures concerning the generation and use of passwords?	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>		

QUESTION DETAIL

Access Control #8

Question: Does the failure of cryptographic module authentication NOT create a denial of service or adversely impact the operational performance of the system?

☒ Mark For Review ID:263

Comments

Frank took the assignment to follow up on this item. We are not certain how it is being handled, but think that th DOS is prevented.

Alternate Description / Justification

Please provide a description, explanation, and/or justification for your alternate answer.

We are not sure on this, but assume that there is a workaround using the new cryptographic software we just bought. Need to check this out. The vendor said that it is covered.

Documents

Document Title:

Cryptographic Guidelines

Add Document

Title	File Name			



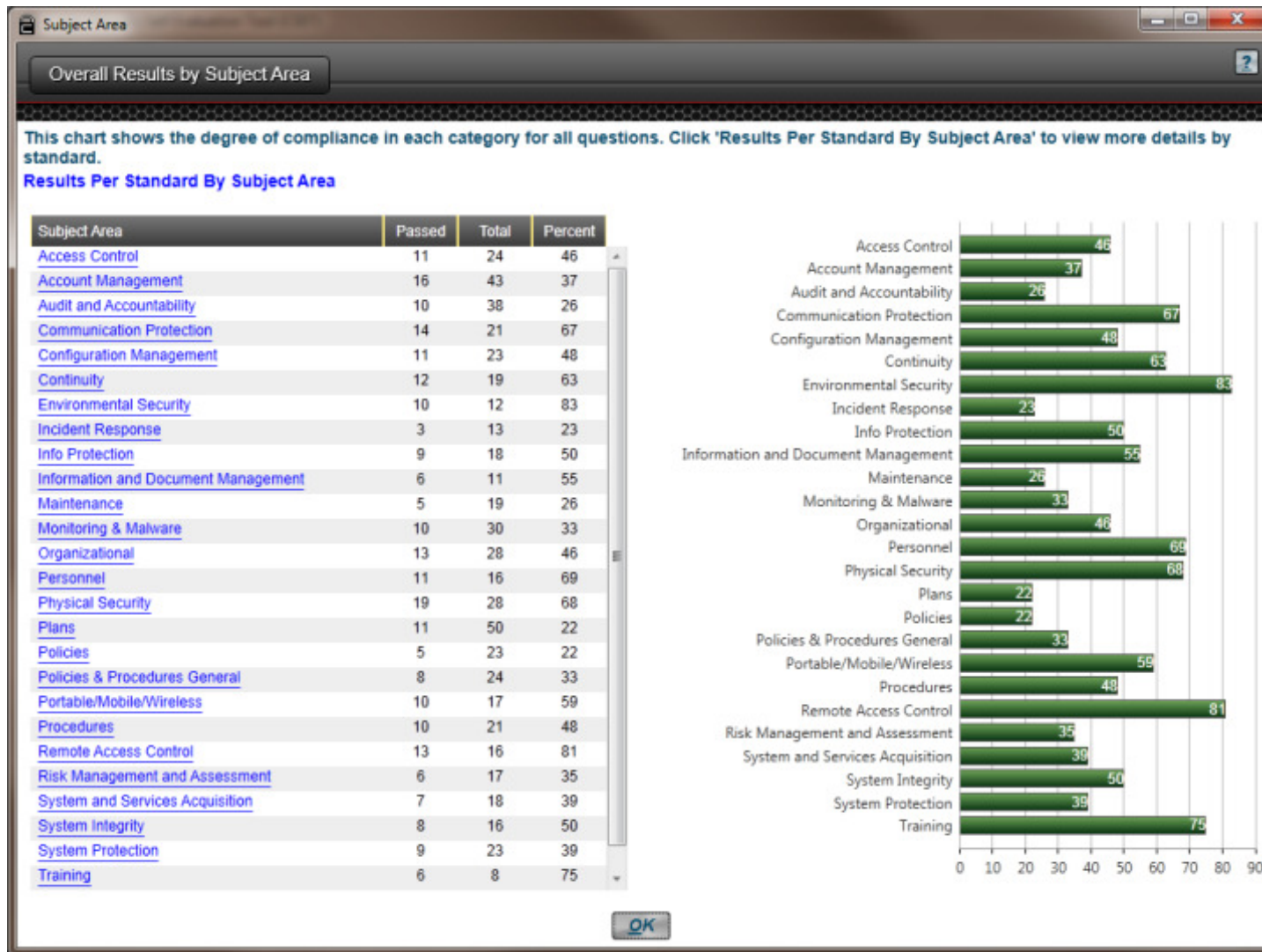
Dashboard Analysis



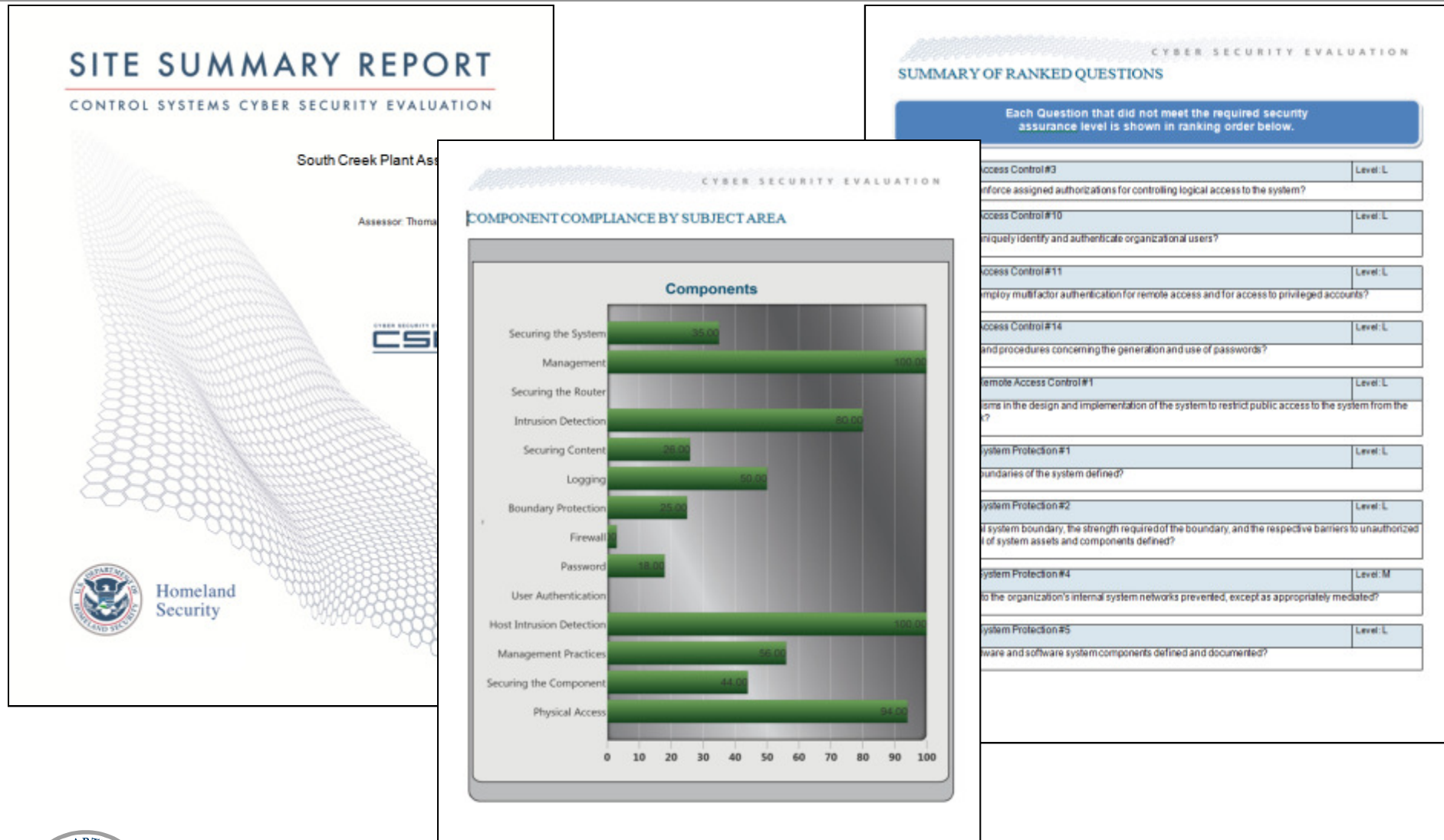
Analysis Detail Screens



Analysis Detail - Example



Hardcopy Reports with Recommendations



Homeland
Security

Resource Library - Search

The screenshot shows a web browser window titled "CSET Resource Library". The page has a dark header with "RESOURCE LIBRARY" in white. Below the header, there's a "Document Tree" sidebar on the left and a main content area on the right. The sidebar contains a search bar with "incident" entered, and a list of search results. The main content area displays the details of the selected document, "Developing an Industrial Control Systems Cybersecurity Incident Response Capability", which is marked as "NONE". Below this, there's a large white box containing the title "Recommended Practice: Developing an Industrial Control Systems Cybersecurity Incident Response Capability" and the date "October 2009". The box also features the Homeland Security logo.

CSET Resource Library

RESOURCE LIBRARY

Document Tree Search

incident

Filter Search Results:

[Incident Response Plan-HHS Template](#)
Resource Library Document

This document provides a Dept. of Health and Human Services (HHS) template for preparing an incident response plan. Downloaded from: <http://www.hhs.gov/ocio/securityprivacy/incidentmanagement/incidentresp.html>.

[ICS Incident Response](#)
Resource Library Document

This recommended practice document from the U. S. Computer Emergency Readiness Team (US-CERT) presents recommendations to help those facilities that use control systems to better prepare for and respond to a cyber incident. Available from <http://www.us-cert.gov>.

[Incident Containment-SANS](#)
Resource Library Document

Form from the SANS Institute Reading Room for intellectual property incident handling - containment. Downloaded from: <http://www.sans.org/score/incidentforms/>.

[Incident Eradication-SANS](#)
Resource Library Document


Developing an Industrial Control Systems Cybersecurity Incident Response Capability

NONE

This recommended practice document from the U. S. Computer Emergency Readiness Team (US-CERT) presents recommendations to help those facilities that use control systems to better prepare for and respond to a cyber incident. Available from <http://www.us-cert.gov>.

Recommended Practice:
Developing an Industrial Control Systems Cybersecurity Incident Response Capability

October 2009

 **Homeland Security**



Homeland
Security

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

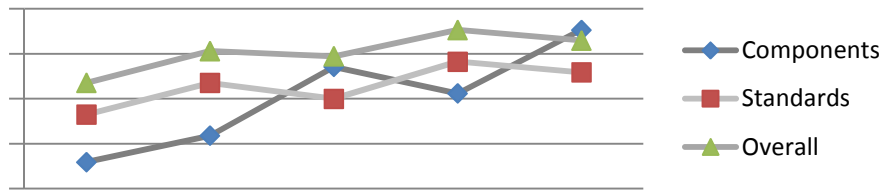
- Merging
- Comparison
- Aggregation
- Trending



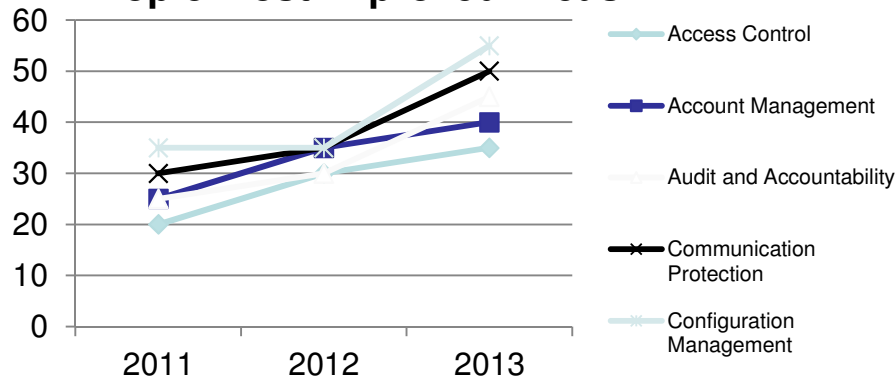
Trending Sample Screen

● CSET Assessment Aggregation -- Trending Mode

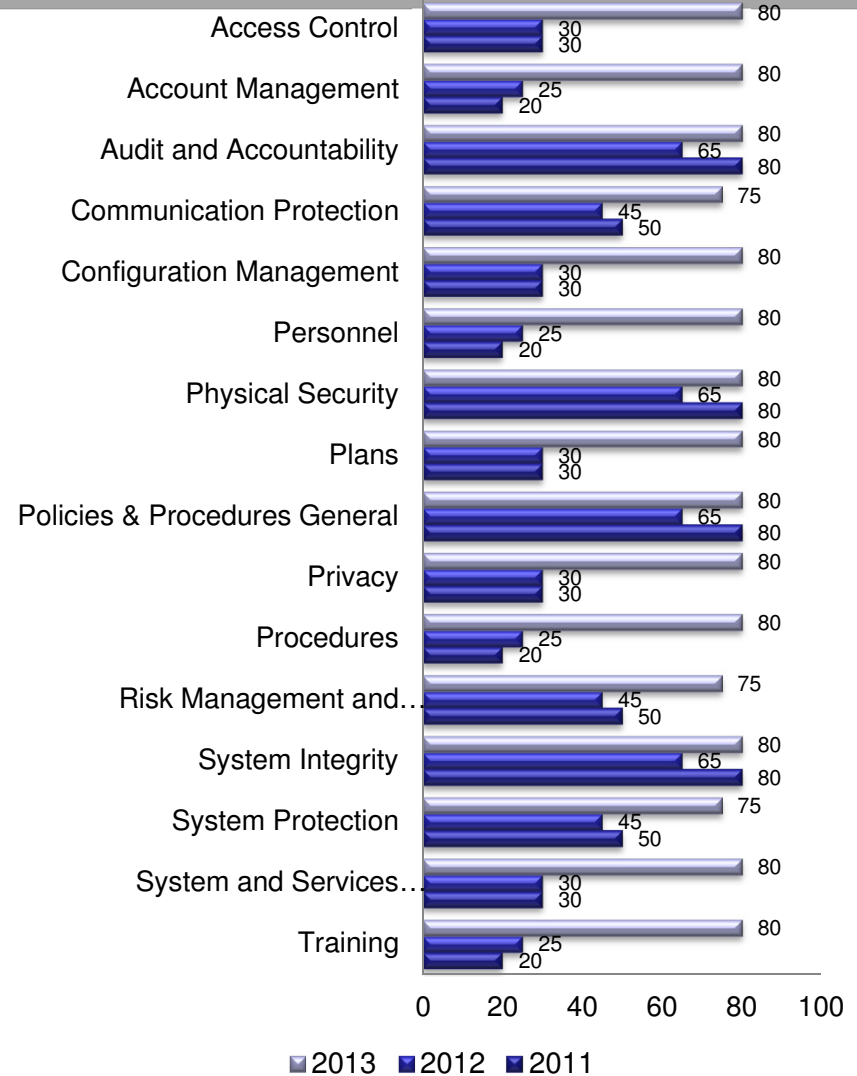
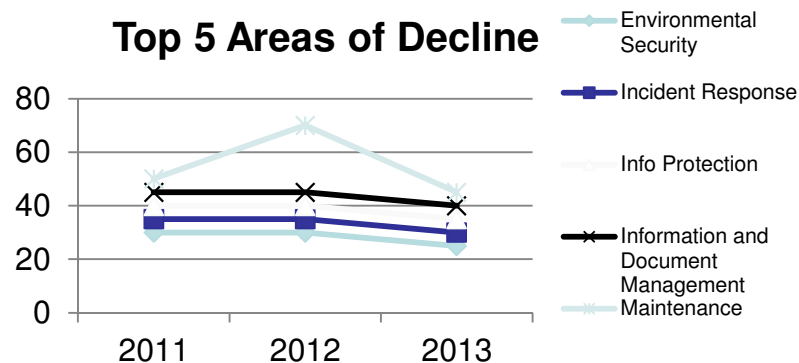
Overall Trends



Top 5 Most Improved Areas



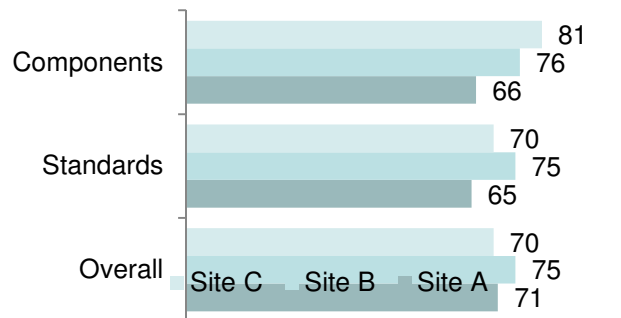
Top 5 Areas of Decline



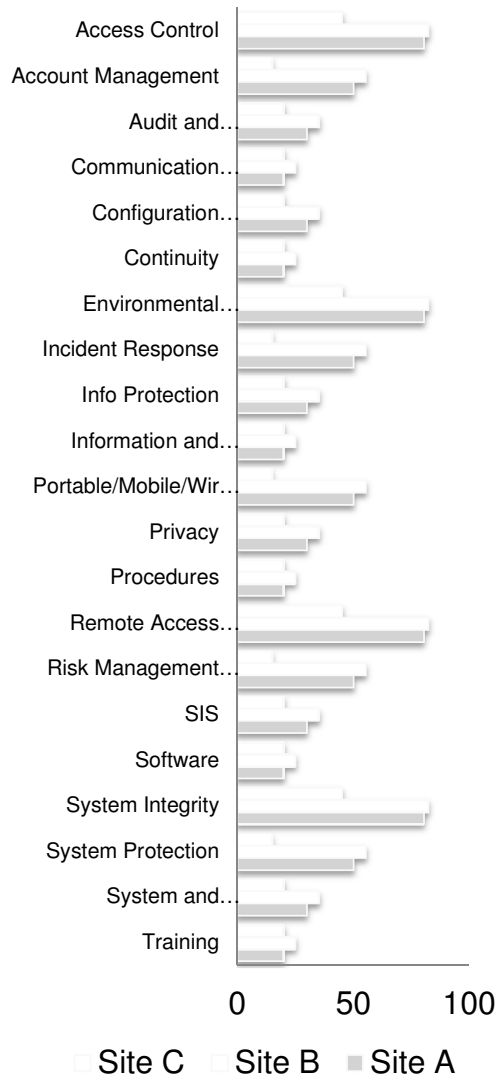
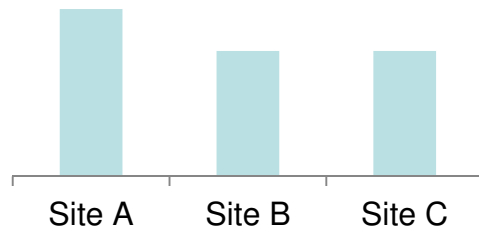
Aggregation Sample Screen

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



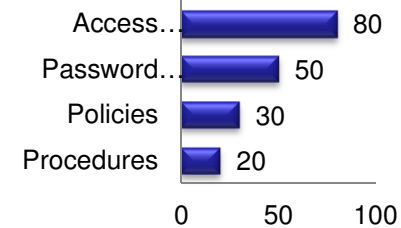
SAL Level



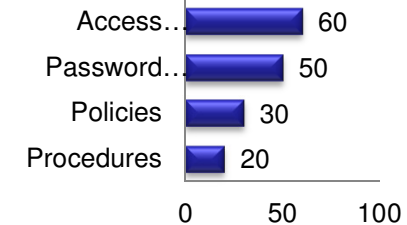
Sort By Best

Sort By Worst

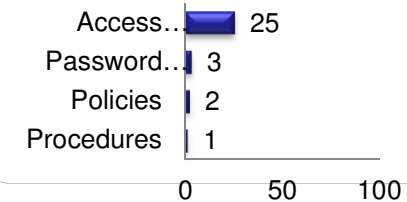
Site A



Site C



Site B



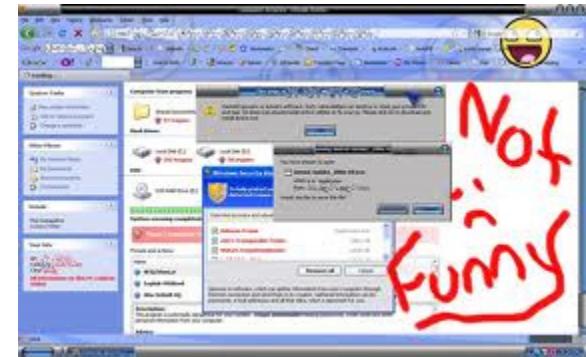
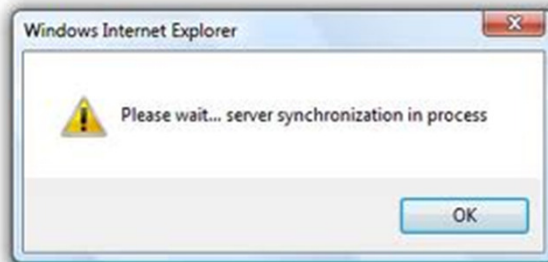
CSET 6.0 Enhancements (cont.)

New/Updated Functionality

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

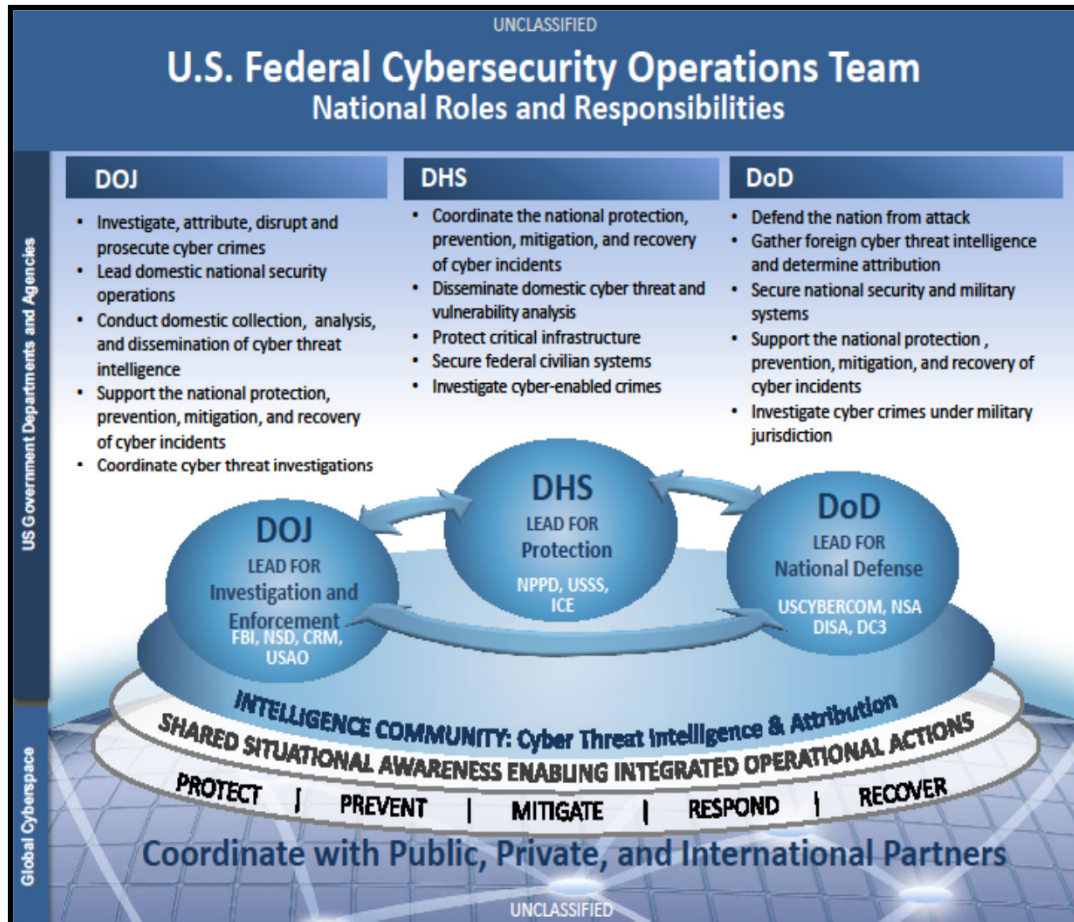


What if Boom?



Homeland
Security

National Cybersecurity Team



Each Department has distinct, yet complementary roles:

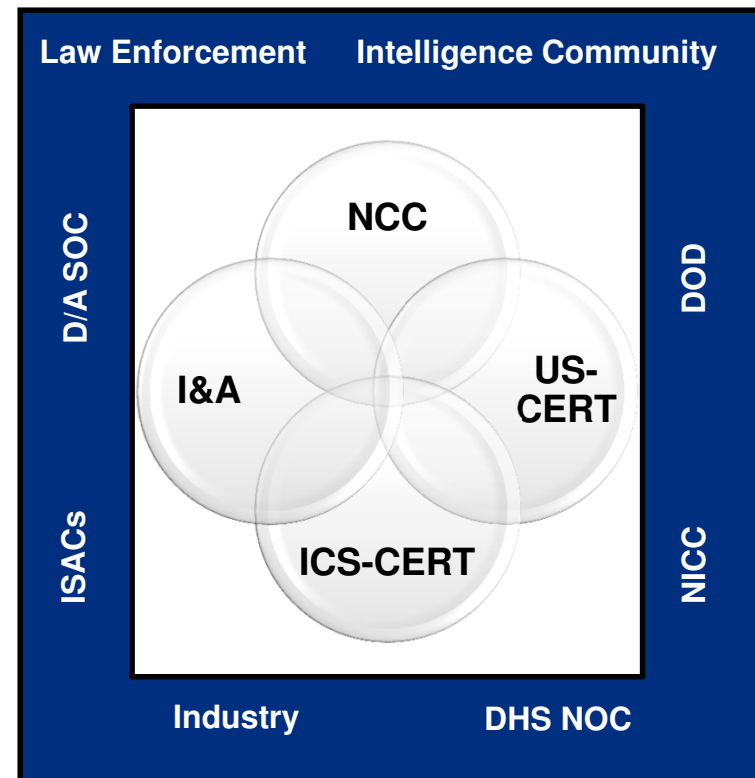
- **DHS:** responsible for coordinating the domestic all-hazards preparedness efforts of executive departments and agencies
- **DOJ:** responsible for responding to domestic counterterrorism, intelligence, and law enforcement activities
- **DOD:** responsible for national defense, foreign cyber intelligence,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



Homeland
Security

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](tel: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>



The screenshot shows the US-CERT AMAC Malware Analysis Submissions web form. At the top is the US-CERT logo and the text "UNITED STATES COMPUTER EMERGENCY READINESS TEAM". Below this is the title "US-CERT AMAC Malware Analysis Submissions". A red box highlights the "Web Disclaimer" section, which contains several paragraphs of legal text regarding the submission of malware artifacts to the Department of Homeland Security's (DHS) United States Computer Emergency Readiness Team (US-CERT). The text states that the submitter agrees to the following: DHS provides analysis and warnings of threats to and vulnerabilities of its systems, as well as mitigation strategies as appropriate; the submitter has obtained the data, including any electronic communications, and is disclosing it to DHS consistent with all applicable laws and regulations; the submitter acknowledges that DHS's analysis is for the purpose of identifying a limited range of threats and vulnerabilities; the submitter understands that DHS makes no warranty that information provided by DHS will detect or mitigate any particular threat or vulnerability; the submitter agrees that the U.S. Government, its officers, contractors, and employees are not liable or otherwise responsible for any damage resulting from the implementation of any guidance provided; the submitter understands that DHS may retain data submitted to it and use it, alone or in combination with other data, to increase its situational awareness and understanding of cybersecurity threats; that DHS may share data submitted to it with other cybersecurity centers in the U.S. Government; that DHS may, from time to time, derive from submitted data certain indicators of malicious activity related to cybersecurity, including but not limited to Internet Protocol (IP) addresses, domain names, file names and hash/digest values; and that DHS may issue warnings to the public about the malicious nature of such indicators, in a way that is not attributable to submitter. Below the disclaimer is a checkbox labeled "I/We agree to the terms above". At the bottom, there are four input fields labeled "First Name", "Last Name", "Organization", and "Open Incident ID".

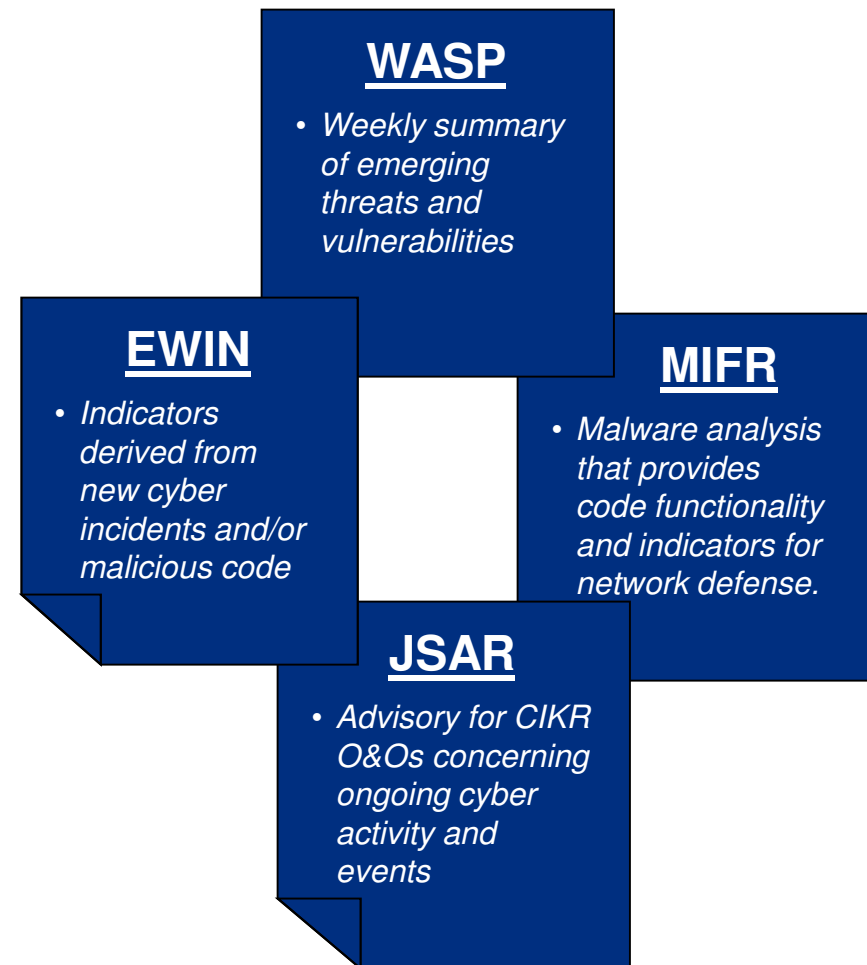


Homeland
Security

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.



Homeland
Security

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 anomalies!



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



Homeland Security



Homeland
Security