



ICS-CERT

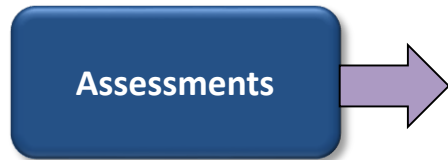
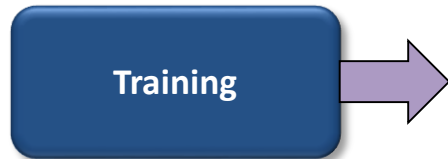
***Jeff Gray – Unit Chief, Training and Outreach***

**Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)  
National Cybersecurity and Communications Integration Center (NCCIC)**

# ICS-CERT Organization

Mission

## Risk Reduction



Assisting critical infrastructure asset owners to reduce the risk of impacts from cyber attacks and events by assisting them to improve their cybersecurity defensive posture and respond to incidents and emerging threats/vulnerabilities.

- ### Benefits
- Awareness of emerging threats
  - State of the art analysis
  - Incident response support
  - Established partnerships
  - Collaboration with other agencies and partners

## Operations



Partners: ISACs, Asset Owners, IC, LE, Agencies, Associations, International

# Assessments: On-Site Support

- ICS-CERT uses the CSET to assist critical infrastructure asset owners in conducting self-assessments
  - 50 assessments in multiple sectors in FY-2010
  - 80 assessments in FY-2011
  - 85 assessments in FY-2012
  - 72 assessments in FY-2013 (#'s affected by sequestration)
  - 46 assessments in FY-2014 (as of May 7, 2014)
- Assessment teams assist infrastructure asset owners in all sectors to identify gaps in their security posture and implement the recommended mitigation strategies
- Architectural reviews and analysis assessments are also available



# Cyber Security Evaluation Tool (CSET<sup>®</sup>)

- Stand-alone software application
- Self-assessment using recognized standards
- Tool for integrating cyber security into existing corporate risk management strategy



## CSET Download:

[us-cert.gov/control\\_systems/csetdownload.html](http://us-cert.gov/control_systems/csetdownload.html)



# Component Questions

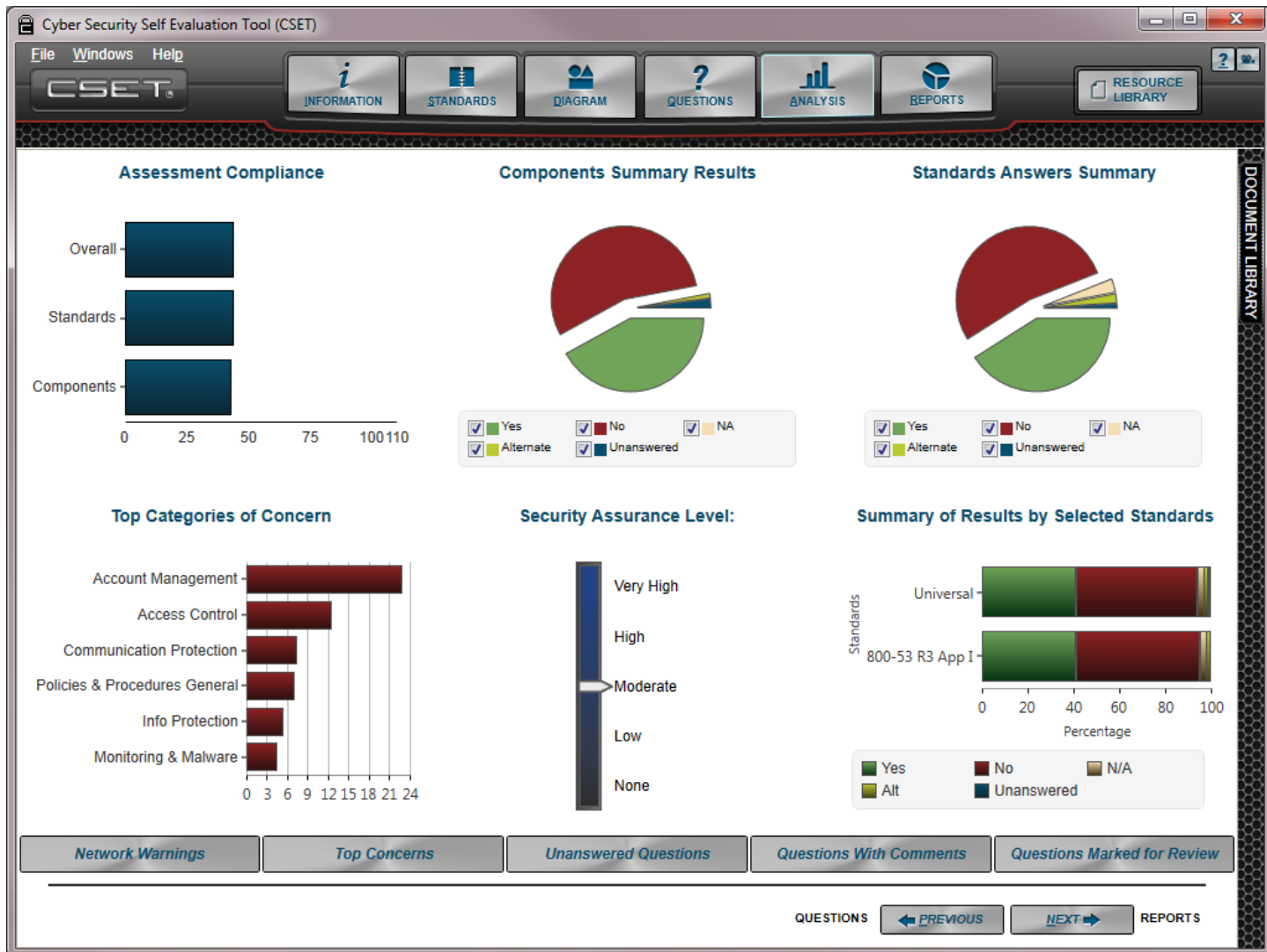
The screenshot displays the CSET Main Window interface. At the top, there is a menu bar with 'File', 'Windows', and 'Help'. Below the menu bar is a toolbar with icons for INFORMATION, STANDARDS, DIAGRAM, QUESTIONS, ANALYSIS, and REPORTS. The main window is divided into three panels:

- QUESTION CATEGORIES:** This panel on the left shows a tree view of question categories. The 'Component Defaults' section is highlighted with an orange box. It includes sub-items like 'Boundary Protection', 'Firewall', 'Host Intrusion Detection', 'Intrusion Detection', 'Logging', 'Management', 'Management Practices', 'Password', 'Physical Access', 'Securing Content', 'Securing the Component', 'Securing the Router', 'Securing the System', and 'User Authentication'. Below this, there are 'Components' including 'Front End Processor' (with sub-item 'FEP-34342' and 'Intrusion Detection'), 'HMI', and 'Operator Workstation'.
- Boundary Protection:** The central panel displays a list of 8 questions. Each question has a status indicator (a colored circle) and an 'Alt' button. The questions are:
  - Are public facing servers placed in a DMZ. In other words, behind a firewall with an additional firewall between that and any systems on the internal network? (Red circle)
  - Have rulesets been reviewed for appropriate order? (Red circle)
  - Have state tables been reviewed? (Red circle)
  - Is all incoming and outgoing ICMP traffic denied except where specifically permitted by your organization. (Green circle)
  - Are loose and strict source routing blocked and logged? (Red circle)
  - Is outbound traffic with an invalid source address blocked? In other words, is egress filtering implemented? (Green circle)
  - Is traffic to your e-mail server only allowed via a specific protocol and port? (Red circle)
  - Is direct external traffic, traffic from the Internet, to critical servers blocked by default? (Red circle)
- QUESTION INFO:** The right panel provides details for the selected question, 'Boundary Protection #1'. It includes a 'Supplemental' section with a paragraph explaining DMZ risks and a 'Level Specific Requirement' section with a question about public facing servers. At the bottom, there is a 'Component Types' table:

Component Type	Action
Application Server	Override
Database Server	Override
Firewall	Override
Web Server	Override



# Analysis Screen



# Hardcopy Reports

## SITE SUMMARY REPORT

CONTROL SYSTEMS CYBER SECURITY EVALUATION

South Creek Base Assessment

1/12/2013

Assessor: John Jakobson Doe

CYBER SECURITY EVALUATION TOOL  
**CSET**  
VERSION 6.1



Homeland Security

### CYBER SECURITY EVALUATION SUMMARY OF RANKED QUESTIONS

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

Rank: 1    Access Control #3    Level: L

Does the system enforce assigned authorizations for controlling logical access to the system?

Rank: 2    Access Control #10    Level: L

organizational users?

Level: L

remote access and for access to privileged accounts?

Level: L

eration and use of passwords?

Level: L

on of the system to restrict public access to the system from the

Level: L

Level: L

quired of the boundary, and the respective barriers to unauthorized defined?

Level: M

networks prevented, except as appropriately mediated?

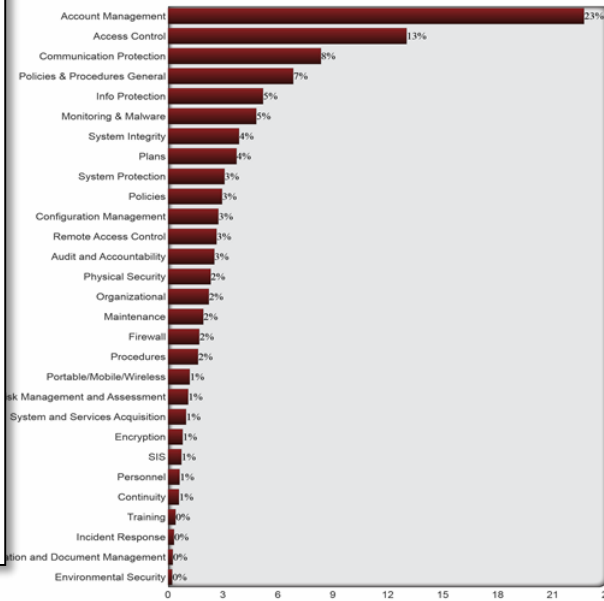
Level: L

ents defined and documented?

### SUBJECT AREAS

shows subject areas needing the most attention. Each bar represents the labeled subject area's weighted contribution so combined total always equals 100%. The weighted contribution includes the importance of both the question and the subject as well as the percentage of missed questions in that subject area.

#### Ranked Subject Areas



# Resource Library

The screenshot displays the CSET Resource Library web application. The interface includes a title bar with the text "CSET Resource Library" and a "Resource Library" button. Below this is a "Document Tree" and "Search" section. The "Document Tree" is expanded to show a list of categories and templates. The categories are "Guidance", "Reports", and "Templates". The "Templates" category is further expanded to show a list of specific templates, each with a small icon. The main content area features a large graphic with a blue hexagonal pattern and images of industrial and infrastructure scenes. The text "Resource Library" is overlaid on the graphic, along with a paragraph of introductory text.

**Document Tree** Search

- Guidance
- Reports
- Templates
  - Cryptography & Encryption
  - Processes & Procedures
  - Access Control
  - Service Providers
  - Wireless
  - Incidents
  - Security Plans
    - Contingency Plan\_IT-HHS Template
    - CyberSec Plan-NRC Template
    - IT Disaster Recovery Plan-FLA Template
    - InfoSec Plan-AbqSPIN Template
    - InfoSec ISS-Neb Template
    - Sec Approach Plan-HHS Template
    - SecPlan-CoSN Template
    - SecPlan\_Major Apps-USG Template
    - SecPlan-LMRs-PSWN Template
    - SecPlan\_Network-QIT Template

**Resource Library**

This library of cyber security standards, reports, and templates are provided for you. Additionally there are several cyber security guides and white papers to assist you with your background in cyber security, determining priorities, and...





# Homeland Security