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

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.

Risk Reduction

- ICSJWG
- Training
- Assessments
- Tools - CSET

Operations

- Incident Response
- Vulnerability Coordination
- Situational Awareness
- Technical Analysis

Benefits

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

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

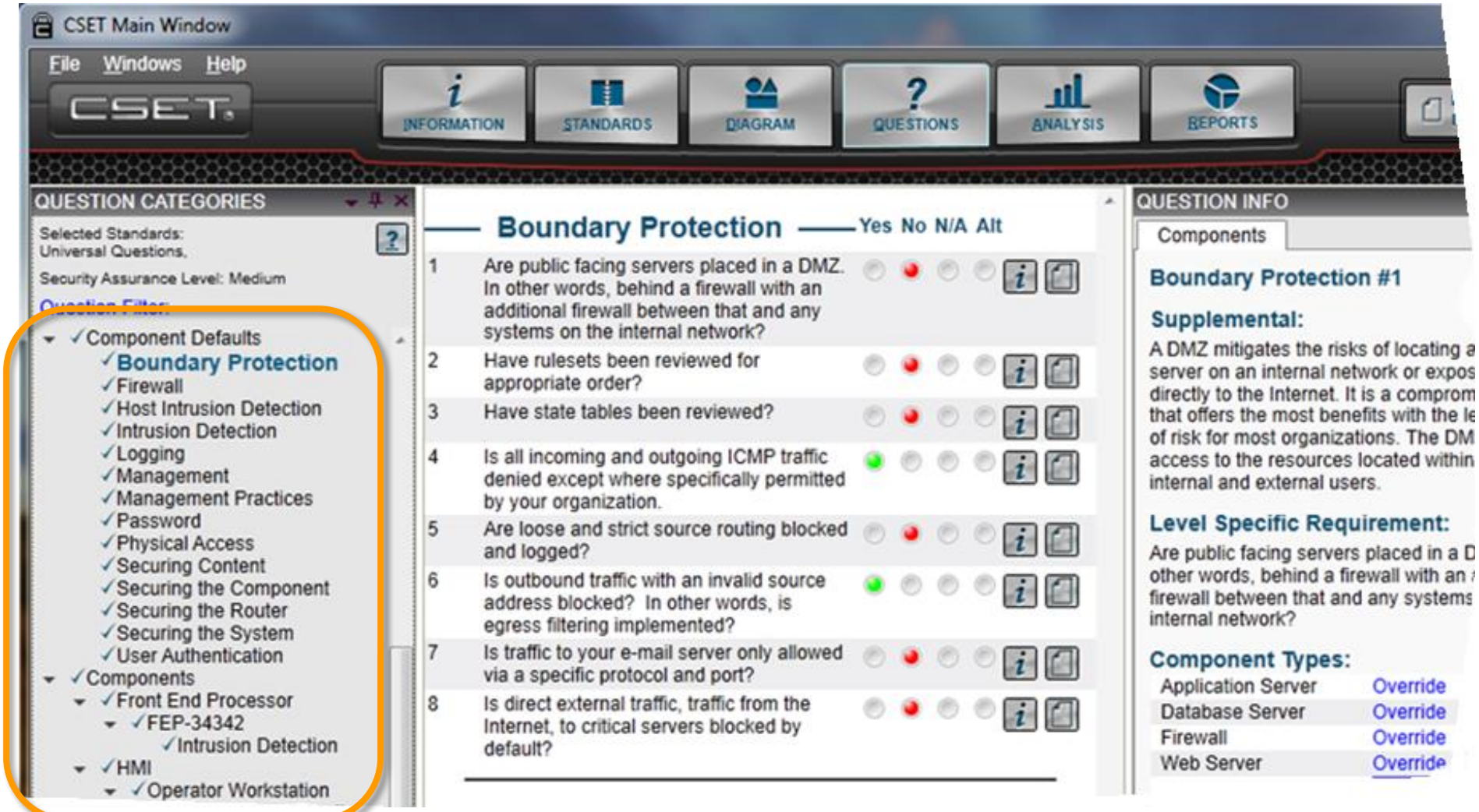
Cyber Security Evaluation Tool (CSET®)

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

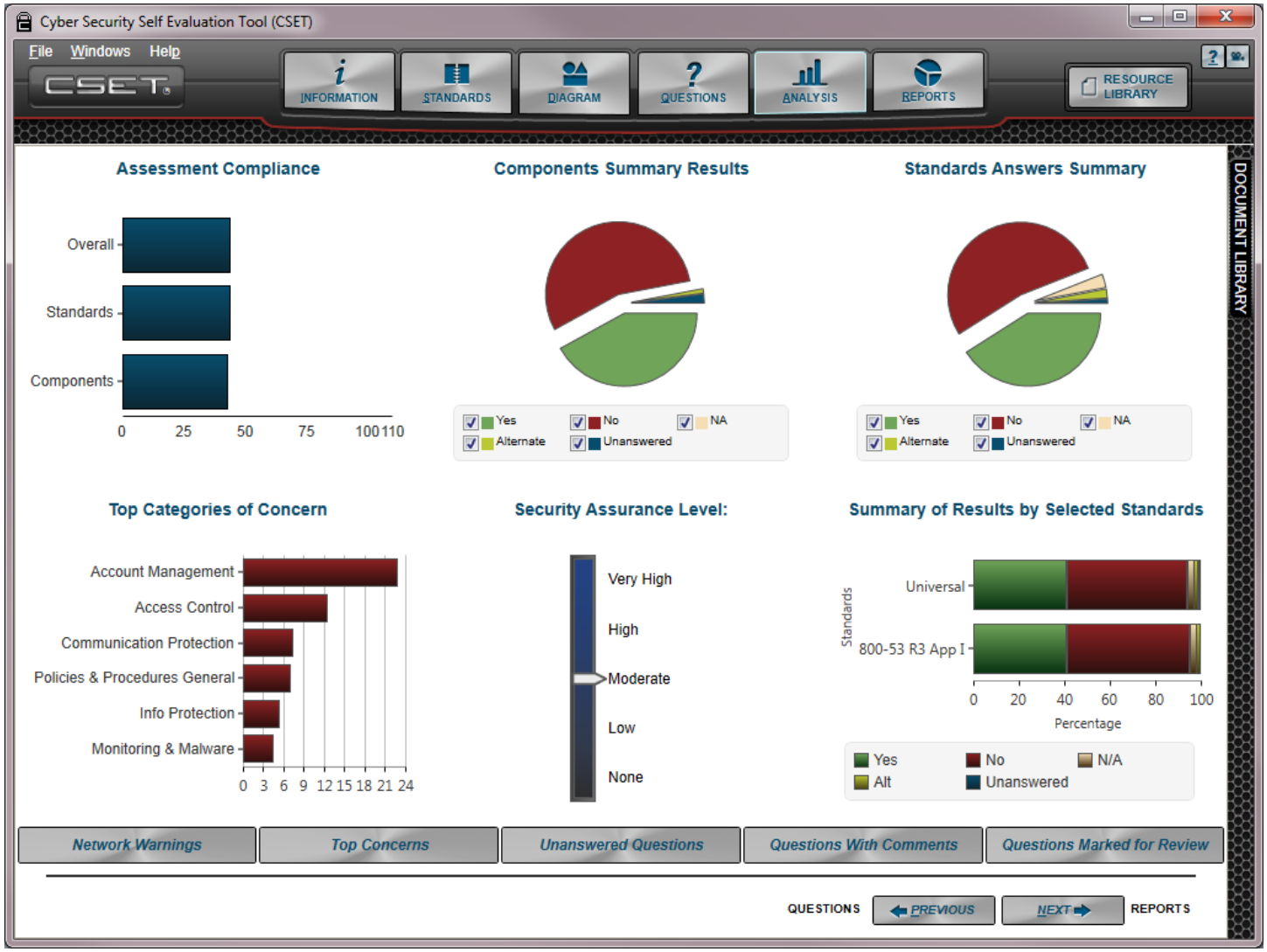
CSET Download:

us-cert.gov/control_systems/csetdownload.html

Component Questions



Analysis Screen



Hardcopy Reports

SITE SUMMARY REPORT

CONTROL SYSTEMS CYBER SECURITY EVALUATION

South Creek Base Assessment

1/12/2013

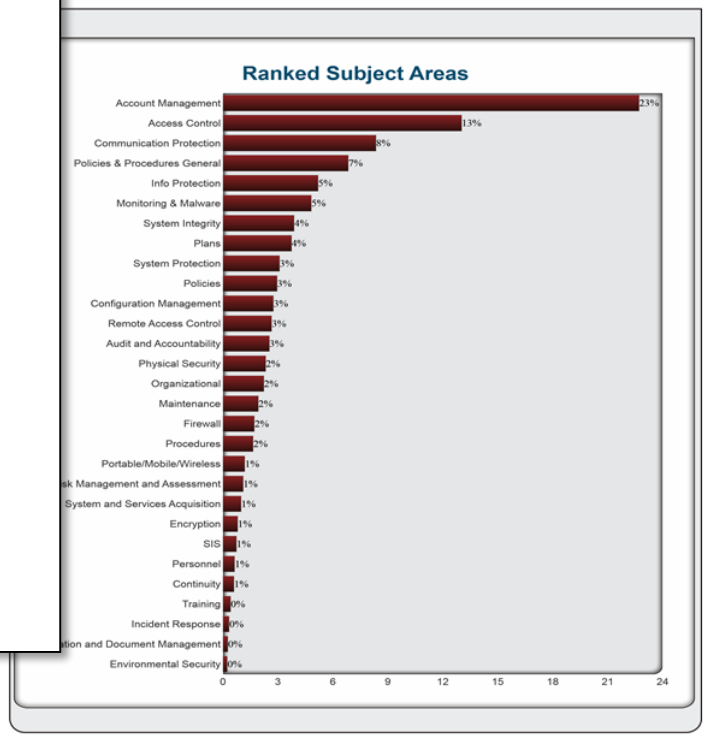
Assessor: John Jakeobson Doe

CYBER SECURITY EVALUATION TOOL
CSET
VERSION 5.1

Homeland Security

SUBJECT AREAS

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

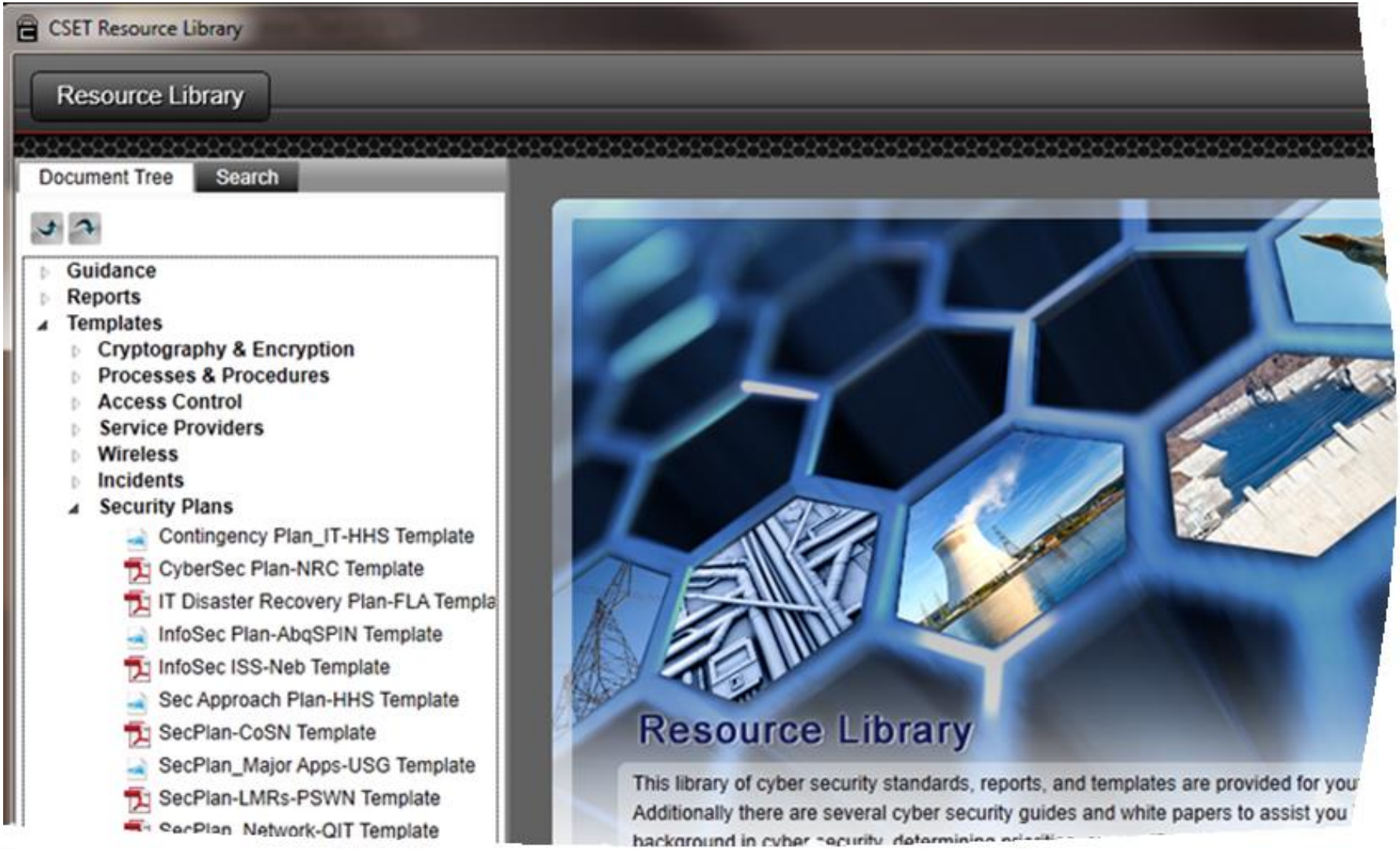


SUMMARY OF RANKED QUESTIONS

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
ganizational 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
uired of the boundary, and the respective barriers to unauthorized defined?		
		Level: M
networks prevented, except as appropriately mediated?		
		Level: L
ents defined and documented?		

Resource Library



Homeland Security