

CHEMICAL SECURITY SEMINARS

Virtual Expo CISA's Cybersecurity Evaluation Tool (CSET)

**Steven Geraldo – Program Manager, Vulnerability
Management Department, CISA
Cybersecurity**

**Randy Woods – Senior CSET Engineer, Idaho
National Laboratory, Department of Energy**



#ChemicalSecurity

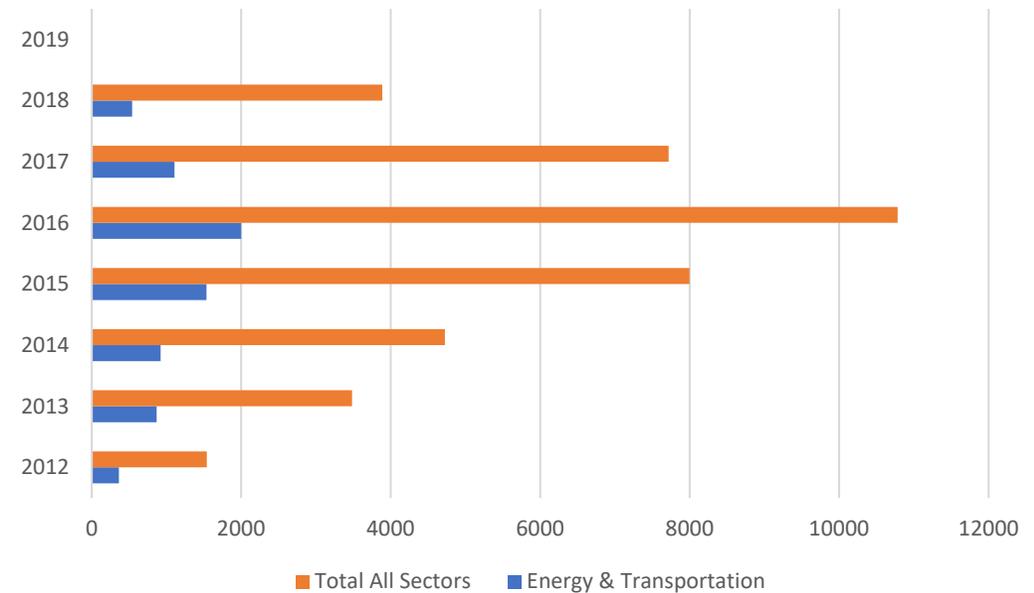
CYBERSECURITY EVALUATION TOOL



CSET Usage

- 14 years
- 41,211 downloads from 2012 -2018
- 10,389 downloads for 2019
- 1,438 downloads for 2020

Energy Sector vs All Downloads





**Where do I start?
Where do I stand now?
What are my priorities?**



CSET Basis

Requirements derived from industry standards

NIST Special Publication 800-53	Recommended Security Controls for Federal Information Systems Revisions 3, 3 Appendix I (ICS Controls), 4, and 4 Appendix J
TSA Pipeline Security Guidelines	Transportation Security Administration (TSA) Pipeline Security Guidelines
NERC Critical Infrastructure Protection (CIP)	Reliability Standards CIP-002 through CIP-009, Revisions 3 and 4 Reliability Standards CIP-002 through CIP-011, Revision 5, Revision 6
DoD Instruction	8500.2 Information Assurance Implementation 8510.01 Risk Management Framework
NIST Special Publication 800-82	Guide to Industrial Control Systems (ICS) Security, Revisions 1 and 2
Nuclear	NRC Reg. Guide 5.71 Cyber Security Programs for Nuclear Facilities NEI 08-09: Cybersecurity Plan for Nuclear Power Reactors
CFATS RBPS 8- Cyber	Chemical Facilities Anti-Terrorism Standard, Risk-Based Performance Standards Guidance 8 – Cyber, 6 CFR Part 27
NIST Cybersecurity Framework	Executive Order 13636, “Improving Critical Infrastructure Cybersecurity,” Cybersecurity Framework V1.1
CNSSI 1253 and Draft ICS Overlay	Committee on National Security Systems Instruction (CNSSI) No. 1253, with Draft Industrial Control Systems Overlay



CSET Capabilities



*What CSET **CAN** do:*

- Provide a consistent means of evaluating a control system network as part of a comprehensive cybersecurity assessment
- Specify cyber security recommendations
- Report using standards-based information analysis
- Provide a baseline cybersecurity posture



*What CSET **CAN'T** do:*

- Validate accuracy of user inputs
- Ensure compliance with organizational or regulatory cybersecurity policies & procedures
- Ensure implementation of cybersecurity enhancements or mitigation techniques
- Identify all known cybersecurity vulnerabilities



Assessment Team



A TEAM of participants is required to perform a successful assessment

Type of Participant	Knowledge
Control Systems Engineer	Control systems
Configuration Manager	Systems management
Operations Manager	Business operations
IT Network Specialist	IT infrastructure
IT Security Officer	Policies & procedures
Risk Analyst or Insurance Specialist	Risk





Assessment Process

Basic steps in the assessment



Free Download

For the latest web application:

<https://github.com/cisagov/cset>

For old desktop versions:

<https://ics-cert.us-cert.gov/Downloading-and-Installing-CSET>



Live Demo



Enter your email address and password to login.

Login

[Forgot Password](#)
[Register New User Account](#)

The Cyber Security Evaluation Tool (CSET®) is a Department of Homeland Security (DHS) product that assists organizations in protecting their key national cyber assets. It was developed under the direction of the DHS National Cybersecurity Assessments and Technical Services team (NCATS) by cybersecurity experts. This tool provides users with a systematic and repeatable approach for assessing the security posture of their cyber systems and networks. It includes both high-level and detailed questions related to all industrial control and IT systems.





Prepare



Diagram



Questions



Results

Assessment Information

Security Assurance Level (SAL)

Cybersecurity Standards Selection

Assessment Information

Details

Assessment Name *

Assessment Date

Facility Name

City Or Site Name

State/Province/Region

Contacts

INEL-NT\HANSBK
INEL-NT\HANSBK@myorg.org
Administrator

Assessment Owner

+ Add Contact

Demographics

Sector

Industry





Prepare



Diagram



Questions



Results

Assessment Information

Security Assurance Level (SAL)

Cybersecurity Standards Selection

Security Assurance Level (SAL)

The Security Assurance Level or SAL determines the number of questions you will need to answer and level of rigor of the assessment. For example, a typical high SAL will contain 350-1000 questions where a low SAL will typically contain 30-350 questions, depending on the selected standard.

Current Security Assurance Level

Overall	Confidentiality	Integrity	Availability
Low	Low	Low	Low

Choose one of the three SAL methodologies below to determine the correct level for your assessment.

Simple

General Risk Based

NIST-60 / FIPS-199

Overall SAL

Low

Moderate

High

Very High

Confidentiality

This value relates to the importance of protecting information from unauthorized access. The more important it is that unauthorized users do not have access to the information the higher your SAL level.

Low

Moderate

High

Very High

Integrity

This value relates to the the importance of the accuracy of information. The more important it is that information is kept consistent, accurate, and only changed by those authorized the higher your SAL level.





Prepare

Diagram

Questions

Results

Assessment Information

Security Assurance Level (SAL)

Cybersecurity Standards Selection

Cybersecurity Standards Selection

Select a standard from the list below to define the questions you will answer during the assessment. Standards in bold text are recommended based on your demographic information.

[I want to do a basic assessment instead](#)

Requirements

25

Questions

57

Chemical, Oil, and Natural Gas

- CFATS Risk-Based Performance Standards Guide 8-Cyber
- INGAA Control Systems Cyber Security Guidelines for the Natural Gas Pipeline Industry
- CIS Controls Version 6

DoDI and CNSSI

- DoD Instruction 8510.01
- CNSSI No. 1253 Baseline V2 March 27, 2014

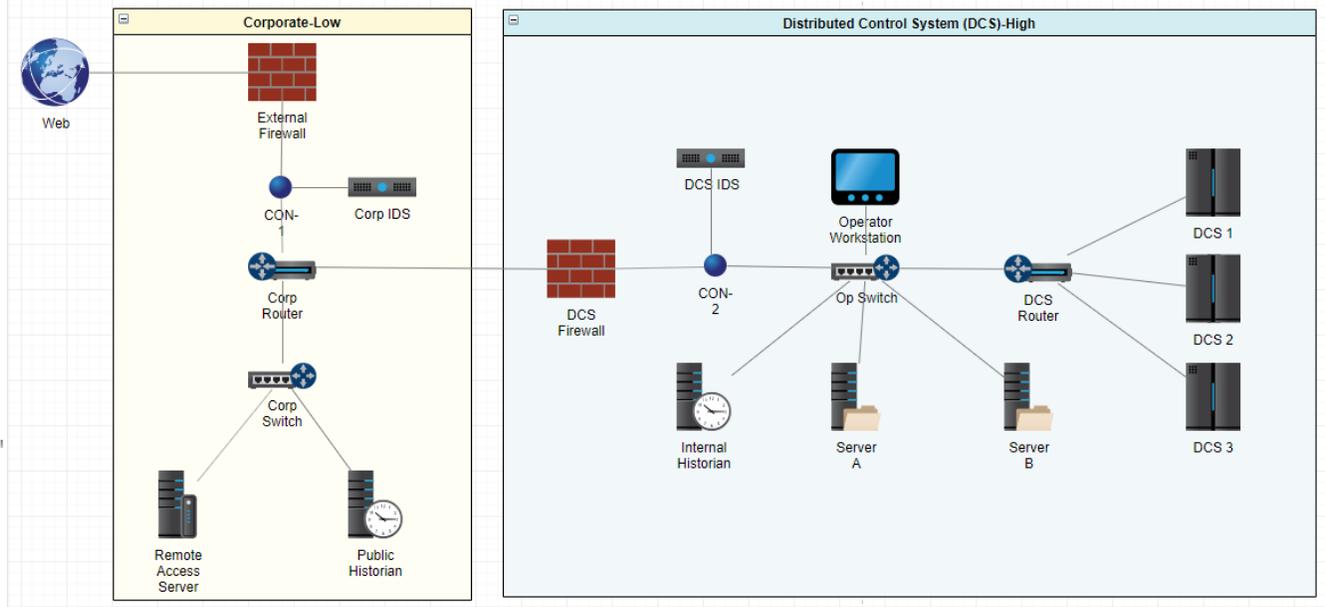
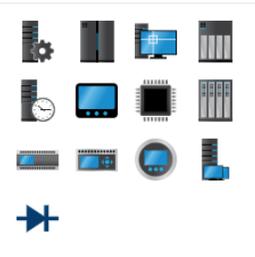
Electrical

- NERC CIP-002 through CIP-009 Rev 3
- NERC CIP-002 through CIP-009 Rev 4
- NERC CIP-002 through CIP-011 Rev 5
- NISTIR 7628 Guidelines for Smart Grid Cyber Security: Vol. 1
- NISTIR 7628 Guidelines for Smart Grid Cyber Security: Vol. 1 Rev 1
- NERC CIP-002 through CIP-014 Rev 6

Financial

- ACET Maturity Assessment





Diagram

View

- Grid 10 pt
- Page View
- Background Image
- Shadow

Options

- Connection Arrows
- Connection Points
- Guides

Paper Size

US-Letter (8.5" x 11")

Portrait Landscape

Clear Default Style



Network Diagram

Steven Geraldo and Randall Woods
December 16, 2020



Prepare

Diagram

Questions

Results

Standard Questions

Access Control

Account Management

Audit and Accountability

Communication Protection

Configuration Management

Continuity

Incident Response

Monitoring & Malware

Organizational

Personnel

Physical Security

Plans

Policies & Procedures General

Procedures

Remote Access Control

Risk Management and Assessment

Safety Instrumented System (SIS)

System and Services Acquisition

Questions Mode

Requirements Mode

Collapse All

Expand All



Auto-load Supplemental

Access Control - Standard Questions

Access Agreements



1 Are appropriate agreements finalized before access is granted, including for third parties and contractors?

Yes No NA Alt



Least Privilege



2 Is the concept of least privilege used to accomplish assigned tasks?

Yes No NA Alt



System Use Notification



Does the organization have any signage or banners indicating system use policies?

Yes No NA



Access Control

Access Agreements

Do you have any access agreements (formal or informal) for third party access to your system? Access agreements include nondisclosure agreements, acceptable use agreements, rules of behavior, operational or service level agreements and conflict-of-interest agreements.

Yes No NA

1 Are appropriate agreements finalized before access is granted, including for third parties and contractors?

Yes No NA Alt

Icons for document, info, chat, list, and lightbulb, followed by a checkbox labeled 'Mark for review'.

Title: 2.3.6

Category: Personnel Security

Security Assurance Level (SAL): Low

Standard Specific Requirement:

The organization completes appropriate agreements for control system access before access is granted. This requirement applies to all parties, including third parties and contractors, who require access to the control system. The organization reviews and updates access agreements periodically.

2 Are access agreements periodically reviewed and updated?

Yes No NA Alt

Icons for document, info, chat, list, and lightbulb, followed by a checkbox labeled 'Mark for review'.





Prepare

Diagram

Questions

Results

Analysis Dashboard

Control Priorities

Standards Summary

Ranked Categories

Results by Category

Components Summary

Ranked Categories

Results by Category

Component Types

Network Warnings

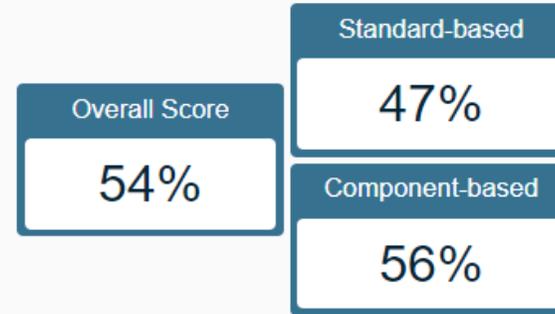
Executive Summary, Overview, & Comments

Reports

Submit Feedback

Analysis Dashboard

Score

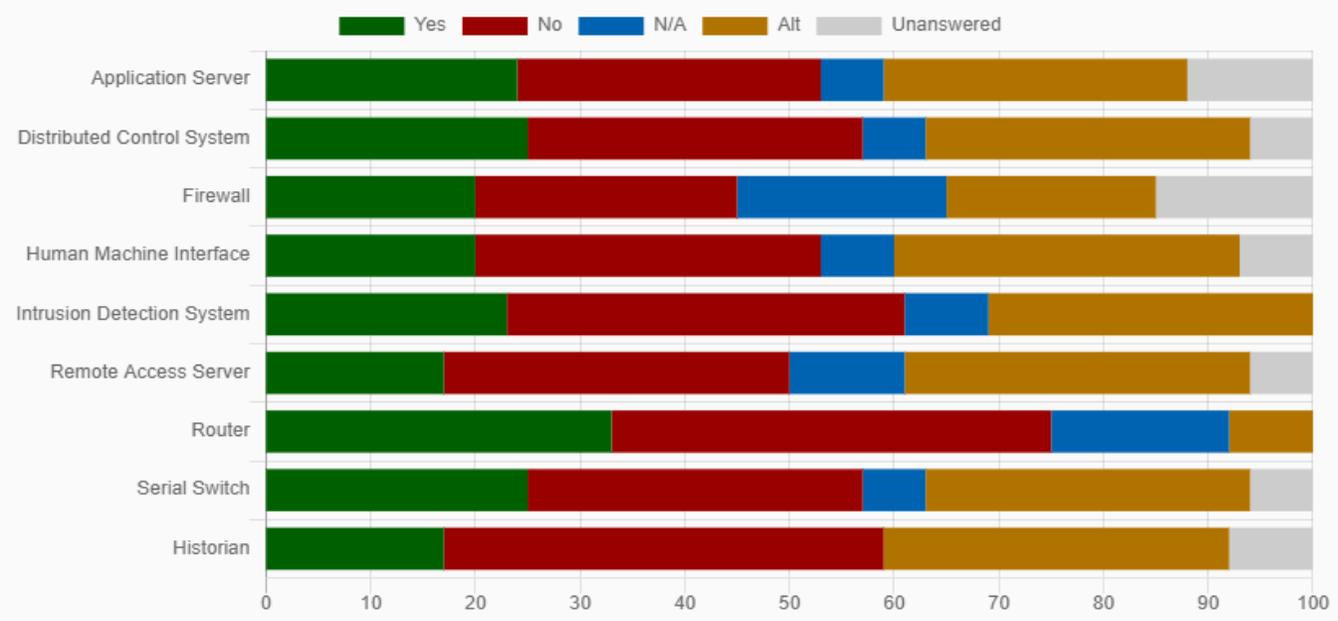


Assessment Compliance



- Analysis Dashboard
- Control Priorities
- Standards Summary
- Ranked Categories
- Results by Category
- Components Summary
- Ranked Categories
- Results by Category
- Component Types
- Network Warnings
- Executive Summary, Overview, & Comments
- Reports
- Submit Feedback

Components By Component Type



Component	Yes	No	N/A	Alternate	Unanswered	Total
Application Server	24%	29%	6%	29%	12%	68
Distributed Control System	25%	32%	6%	31%	6%	144
Firewall	20%	25%	20%	20%	15%	80
Human Machine Interface	20%	33%	7%	33%	7%	15

Steven Geraldo and Randall Woods
December 16, 2020





Prepare

Diagram

Questions

Results

Analysis Dashboard

Control Priorities

Standards Summary

Ranked Categories

Results by Category

Components Summary

Ranked Categories

Results by Category

Component Types

Network Warnings

Executive Summary, Overview, &
Comments

Reports

Submit Feedback

Report Builder

Create your final reports. You can add descriptions, comments, and an executive summary to your reports. You can also specify comments and descriptive text.

[Executive Summary](#)[Site Summary Report](#)[Site Cybersecurity Plan](#)[Site Detail Report](#)[Observations Tear-Out Sheets](#)

Back

Next



Resource Library

Guidance

- > Access Control
- > Acquisition
- > Auditing & Assessment
- > Categorization
- > Cloud Computing
- > Communications
- > Configuration Management
- ∨ Control System Security

21 Steps To Improve Cyber Security

This document from the U. S. Dept. of Energy (DOE) provides specific actions to be taken to increase the security of SCADA networks. Available from <http://www.us-cert.gov>.

Australian Strategies to Mitigate Cyber Intrusions

This document provides information about comparative mitigation implementation costs and user resistance levels to help organisations select the best set of strategies for their requirements.

Catalog of Recommendations V7

This catalog presents a compilation of practices that various industry bodies have recommended to increase the security of control systems from both physical and cyber attacks. The recommendations in this catalog are grouped into 19 families, or categories, that have similar emphasis.

CNSSI 1253 National Security Systems

This Instruction serves as a companion document to NIST SP 800-53 for organizations that employ NSS. It establishes the processes for categorizing NSS and the information they process and for appropriately selecting security controls for NSS from NIST SP 800-53. This Instruction applies to all components of NSS. For NSS, where differences between the NIST documentation and this Instruction occur, this Instruction is authoritative.



[Home](#) » [Module Detail](#)

Module Detail

A Module may be based on an industry standard, or may simply be a collection of questions. Modules based on standards will normally take the Requirements path in order to transfer the requirements into the Set.

If you are building a Standard, manage the requirements by clicking [Requirements](#). The [Questions](#) path will show the structure of the related questions when in 'questions mode' of the assessment.

It is a good practice to attach any related documents to the Module. Click [Manage Documents](#) to upload and attach files.

Module Name *

Short Name *

Description *

Category

[Requirements](#)[? Questions](#)[Manage Documents](#)[« Back to Module List](#)

Import New Module (Question/Requirements Set)

Export

Catalog of Recommendations Rev 7

XML

JSON

Load to editor

CFATS Risk-Based Performance Standards Guide 8-Cyber

XML

JSON

Load to editor

CNSSI No. 1253 (ICS) Overlay Version 1

XML

JSON

Load to editor

CNSSI No. 1253 Baseline

XML

JSON

Load to editor

CNSSI No. 1253 Baseline V2 March 27, 2014

XML

JSON

Load to editor

CNSSI No. 1253 Industrial Control System (ICS) Overlay

XML

JSON

Load to editor

Consensus Audit Guidelines (CAG)

XML

JSON

Load to editor

Control Correlation Identifier Specification V2 release

You must correct all errors before submitting the module for processing.

Module Code

JSON

XML

Schema: XML | JSON

Please specify the code for your new module below. You can either begin typing below, drop a file onto the editor, load an existing module, or copy and paste text below. To get suggestions, type CTRL-Spacebar.

```

1  {
2  "Name": ""
3  "ShortName": ""
4  "Category": ""
5  "Summary": ""
6  "Requirements":[
7  {
8  "Identifier": ""
9  "Text": ""
10 "Heading": ""
11 "Subheading": ""

```

Validation messages

Line 2, Column 10 - String is shorter than the minimum length of 1.
 Line 3, Column 15 - String is shorter than the minimum length of 1.
 Line 4, Column 14 - String is shorter than the minimum length of 1.
 Line 4, Column 14 - Value is not accepted. Valid values: "Chemical, Oil, and Natural Gas", "Custom", "DoDI and CNSSI", "Electrical", "General", "Health Care", "Information Technology", "NIST Framework", "Nuclear", "Process Control and SCADA", "Questions Only",

Supporting Documents

Any additional documents that are referenced by your module need to be added below by dropping the file onto the drop area.

Drop reference files here

Submit



Home

Standard And Question Set Builder

This tool allows you to define your own custom standard or question set for an assessment.

[+ Create Module](#)

[800-53 Revision 7](#)

[Question Set 17-A](#)

[Branch Office Working Standard 1.7](#)





For the latest web application:
github.com/cisagov/cset

For old desktop versions:
ics-cert.us-cert.gov/Downloading-and-Installing-CSET

Questions?

Email: CSD_VM_Methodology@cisa.dhs.gov