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

<table>
<thead>
<tr>
<th>Year</th>
<th>Total All Sectors</th>
<th>Energy &amp; Transportation</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2013</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2014</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2015</td>
<td>4000</td>
<td>2000</td>
</tr>
<tr>
<td>2016</td>
<td>6000</td>
<td>4000</td>
</tr>
<tr>
<td>2017</td>
<td>8000</td>
<td>6000</td>
</tr>
<tr>
<td>2018</td>
<td>10000</td>
<td>8000</td>
</tr>
<tr>
<td>2019</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Where do I start?
Where do I stand now?
What are my priorities?
# CSET Basis

**Requirements derived from industry standards**

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

<table>
<thead>
<tr>
<th>Type of Participant</th>
<th>Knowledge</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control Systems Engineer</td>
<td>Control systems</td>
</tr>
<tr>
<td>Configuration Manager</td>
<td>Systems management</td>
</tr>
<tr>
<td>Operations Manager</td>
<td>Business operations</td>
</tr>
<tr>
<td>IT Network Specialist</td>
<td>IT infrastructure</td>
</tr>
<tr>
<td>IT Security Officer</td>
<td>Policies &amp; procedures</td>
</tr>
<tr>
<td>Risk Analyst or Insurance Specialist</td>
<td>Risk</td>
</tr>
</tbody>
</table>
Assessment Process

Basic steps in the assessment

- Organize the Team
- Determine the Security Assurance Level
- Select Standards and Mode
- Answer Questions
- Analyze Results
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

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.
Assessment Information

Details

Assessment Name: New Assessment
Assessment Date: 10/31/2019

Facility Name

City Or Site Name
State/Province/Region

Contacts

INEL-NTHANSBK
INEL-NTHANSBK@myorg.org
Administrator

Assessment Owner

+ Add Contact

Demographics

Sector
Industry
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 whereas a low SAL will typically contain 30-350 questions, depending on the selected standard.

Current Security Assurance Level

<table>
<thead>
<tr>
<th>Overall</th>
<th>Confidentiality</th>
<th>Integrity</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
</tbody>
</table>

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

- Simple: General Risk Based
- NIST-80 / 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.
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

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

DoD 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
Network Diagram
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

Assessment

Steven Geraldo and Randall Woods
December 16, 2020
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.

1. Are appropriate agreements finalized before access is granted, including for third parties and contractors?
   - 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
Components By Component Type

<table>
<thead>
<tr>
<th>Component</th>
<th>Yes</th>
<th>No</th>
<th>N/A</th>
<th>Alternate</th>
<th>Unanswered</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Server</td>
<td>24%</td>
<td>29%</td>
<td>6%</td>
<td>29%</td>
<td>12%</td>
<td>68</td>
</tr>
<tr>
<td>Distributed Control System</td>
<td>25%</td>
<td>32%</td>
<td>6%</td>
<td>31%</td>
<td>6%</td>
<td>144</td>
</tr>
<tr>
<td>Firewall</td>
<td>20%</td>
<td>25%</td>
<td>20%</td>
<td>20%</td>
<td>15%</td>
<td>80</td>
</tr>
<tr>
<td>Human Machine Interface</td>
<td>20%</td>
<td>33%</td>
<td>7%</td>
<td>33%</td>
<td>7%</td>
<td>15</td>
</tr>
</tbody>
</table>
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
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 organizations 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.
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 *

A Company Custom Extension to the NIST Framework

Short Name *

ACME Custom

Description *

There are some additional questions both specific to our company and that we believe are not generally addressed that we would like to include in all our assessments

Category

Information Technology
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