



# USER MANUAL

The Cyber Security Evaluation Tool (CSET®), Version 9.0.

User Manual

October 2018

This product was developed by the United States Department of Homeland Security (DHS).

## Table of Contents

Introduction to CSET .....	5
Introduction .....	6
Overview .....	8
Disclaimer.....	13
System Basics .....	14
System Requirements.....	14
Installation Procedure .....	15
Stand-alone Install.....	15
Using the Stand-alone.....	23
Enterprise Install .....	25
Evaluation Preparation.....	29
Register a User Account.....	31
Import/Export a CSET Assessment.....	34
Importing a .csetw File .....	34
Importing a .cset File .....	35
Exporting a CSET Assessment .....	36
Custom Questionnaires .....	37
Using the Import New Module.....	37
Title Bar.....	41
Tools Menu.....	43
Assessment Documents .....	45
Parameter Editor.....	46
Protected Features.....	49
Export to Excel.....	51
Resource Library .....	52
Search Screen .....	53
Browse Screen .....	56
User Profile .....	60
User Profile.....	62
Change Password.....	63
Help Menu .....	64
Accessibility Document.....	66
Keyboard Shortcuts.....	67
Terms of Use .....	68
About CSET .....	69
Advisory .....	71
Operation Menus.....	72
Preparation Menu.....	72

Questions Menu .....	74
Results Menu .....	76
Main CSET Window Sections .....	78
Prepare Section.....	78
CSET Landing Page.....	78
Assessment Details.....	79
Contacts Management.....	81
Sector and Demographic Information Screen.....	85
Security Assurance Level (SAL) Selection .....	87
Standard SAL Selection.....	87
General SAL Selection.....	90
General SAL – Injury.....	93
General SAL - Hospital.....	94
General SAL - Death .....	95
General SAL - Capital Assets .....	96
General SAL - Economic Impact .....	97
General SAL - Environmental Cleanup.....	98
General SAL Considerations .....	99
FIPS 199 SAL Selection .....	104
Cybersecurity Standard Selection.....	110
CSET Standards and Groupings.....	113
C2M2 Maturity Indicator Levels.....	123
CFATS Tiers .....	124
Cybersecurity Framework Description.....	125
Framework Implementation Tiers.....	131
Mode Selection .....	133
Assessment Modes.....	134
Assessment Section.....	137
Assessment Screen.....	137
Assessment Modes.....	140
Assessment Screen Questions Mode .....	141
Assessment Screen Requirements Mode.....	142
Assessment Categories .....	143
Question Details, Resources, and Comments .....	145
Details Section Question Mode .....	148
Details Section Requirements Mode.....	150
Supplemental Section .....	151
Comments Section .....	152
Documents Section.....	154
Questions List .....	156

References Section .....	157
Discoveries Section .....	158
Question Discoveries .....	159
Question Filter .....	162
Results Section .....	164
Analysis Screen .....	164
Dashboard in Questions/Requirements Mode .....	167
Ranked Questions .....	169
Overall Ranked Categories .....	172
Standards Analysis .....	174
Standards Summary .....	174
Standards Ranked Categories .....	174
Standards Results By Category Single Standard .....	177
Standards Results by Category Multiple Standards .....	178
Category Rankings .....	179
Reports Section .....	182
Executive Summary, Overview, and Comments Screen .....	182
Report Builder .....	183
Executive Summary Report .....	185
Site Summary Report .....	187
Site Detail Report .....	190
Site Cyber Security Plan .....	191
Discoveries Tear Out Sheets .....	193
Initiation Scenarios .....	194
Glossary .....	199
Frequently Asked Questions (FAQs) .....	205
CSET Revision History .....	207

## Introduction to CSET

This section will help the user better understand the Cyber Security Evaluation Tool (CSET®), its background, and purposes.

# Introduction

The Cyber Security Evaluation Tool (CSET®) provides the following:

1. A framework for analyzing cybersecurity vulnerabilities associated with an organization's overall industrial control system (ICS) and information technology (IT) architecture;
2. A consistent and technically sound methodology to identify, analyze, and communicate to security professionals the various vulnerabilities and consequences that may be exploited by cyber means;
3. The means for the user to document a process for identifying cybersecurity vulnerabilities; and
4. Suggested methods to evaluate options for improvement based on existing Standards and recommended practices.

## Background

The Department of Homeland Security (DHS) developed CSET for asset owners with the primary objective of reducing the risk to the nation's critical infrastructure. Control systems are defined as electronic devices that control physical processes and as such, are a crucial element in the protection of our nation's infrastructure.

CSET is a web-based tool that guides users through a step-by-step process to collect facility-specific information addressing topics such as hardware, software, administrative policies, and user obligations. It then compares that information to relevant security Standards and regulations, assesses overall compliance, and provides appropriate recommendations for improving cybersecurity posture. The tool pulls its recommendations from a collection of the best available cybersecurity Standards, guidelines, and practices. Where appropriate, recommendations are linked to a set of actions that can be applied to enhance cybersecurity controls.

## Objectives and Benefits

The primary objective of CSET is to reduce the risk of cyber attacks by identifying potential cybersecurity vulnerabilities within a system or an organization. CSET implements a simple, transparent process that can be used effectively by all sectors to perform an evaluation of any network. It offers the following benefits:

- Provides a repeatable and systematic approach for assessing the cybersecurity posture of a system, network, site, or facility.
- Provides a comprehensive evaluation and comparison to existing industry Standards and regulations.
- Combines the ICS and IT security knowledge and experience of many organizations.

- Assists in the identification of potential vulnerabilities in the network design and security policies.
- Provides guidelines for cybersecurity solutions and mitigations.
- Provides access to a centralized repository of cybersecurity requirements.
- Provides an opportunity for dialogue on security practices within the user's facility.

## Limitations of this Tool

The tool has a component focus rather than a system focus. Therefore, network architecture analyses, including network hardware and software configuration analyses, will be limited to the extent that they are defined by programmatic and procedural requirements.

CSET is not a risk analysis tool; it will not create a detailed risk assessment.

Most importantly, CSET is only one component of a comprehensive control system security program. A security program based on a CSET assessment alone must never be considered complete or adequate.

## User Qualifications

CSET assessments cannot be completed effectively by any single individual. A cross-functional team consisting of representatives from multiple company areas is essential. The representatives must be subject matter experts with significant expertise in their respective areas. No one individual has the span of responsibility or knowledge to be able to fully and accurately answer all the questions provided by the CSET tool.

## Overview

The Cyber Security Evaluation Tool (CSET®) is a software tool for performing cybersecurity assessments of an organization's enterprise and industrial control cyber systems. It was designed to help asset owners identify vulnerabilities and improve the organization's overall cybersecurity posture by guiding them through a series of questions that represent network security requirements and best practices. The presented requirement questionnaires are based on selected industry Standards, common requirements, and the network diagram (or network topology and architecture).

## CSET Framework

The underlying framework for CSET includes:

- Analysis and user interface tools to assist in the evaluation of an ICS,
- A knowledge base of ICS cybersecurity requirements, regulations, and practices, and
- A collection of solutions to help mitigate vulnerabilities.

## Basic Evaluation Process

### Form the Assessment Team

Prior to beginning the assessment, form a subject matter expert team. Teams typically include representation from senior management, business, operations, IT, ICS, and security. The assembled team is responsible for determining the evaluation levels and answering specific, detailed questions on the control system and security configuration.

Familiarity with the tool will improve and speed up the assessment process. Anyone in the organization who has had training or experience with the tool should be included on the team. Alternately, the primary user should spend some time using the tool with test-only or dummy data prior to commencement of the team activity.

Documents that may be referenced should be gathered prior to the assessment. Useful reference materials include information relating to operations, maintenance, physical security, cybersecurity, and hazardous materials.

### Register for a CSET Account

Register for CSET by first installing CSET. The CSET installation will be on your local desktop. If it is installed locally click the icon to start, if your CSET installation is an Enterprise or company installation see your company CSET administrator for the URL.

After installation navigate to the CSET home page. Below the login is a link that says "Register New User Account". See more on registering a new account at [Register a User Account](#). A new assessment can be started from the user's landing page by clicking the "Start New Assessment"

button.

New Assessment

Figure: New Assessment button

## Add Site Information

Begin the assessment by filling out assessment details. This includes the assessment name and date, information on the subject system, points of contact, and a description of the assessment. Such information will be helpful when referring to the assessment months or years later.

For more information, see the [Assessment Details](#) help section.

The Figure below graphically depicts the next steps of the self-assessment process. A brief summary of the steps is provided below.

# New Navigation Approach

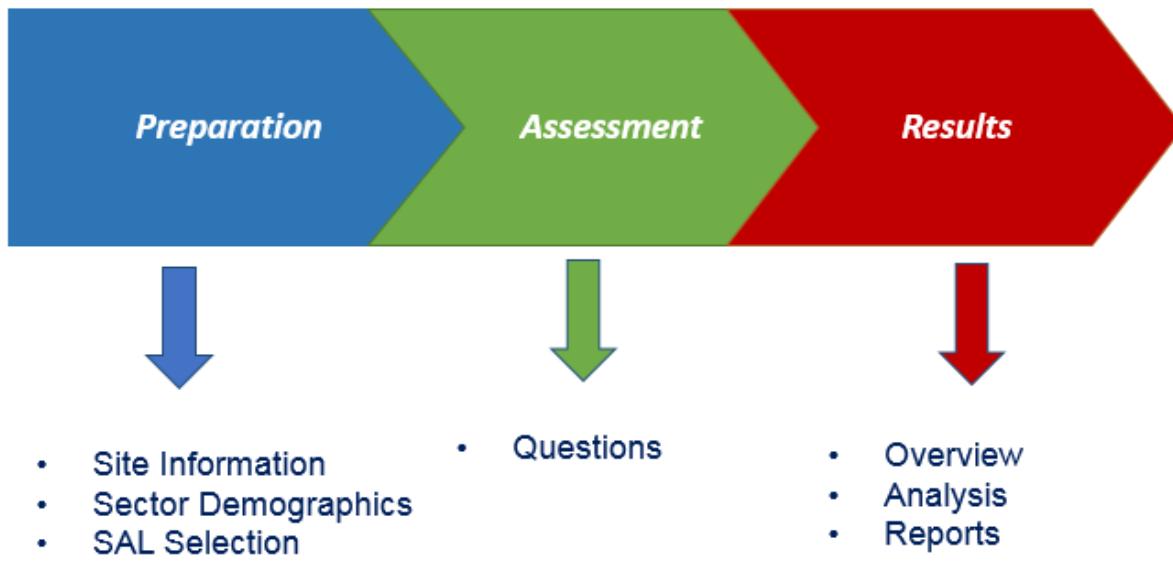


Figure: CSET Process

## Preparation

### **Site Information**

The first part of the assessment preparation process is to provide specific information about the assessment including who was responsible, when it occurred, what sites or facilities were involved, and both descriptive and summary information.

### **Sector Demographics**

CSET collects sector and demographic information to help the user identify the appropriate

Standards and questions that will be presented on the assessment.

## Diagram Components

Not supported in CSET 9.0. This feature will be available in a future release.

### SAL Selection

The system requires that the user identify a security assurance level (SAL), and multiple options are provided to determine what the SAL should be. The user may bypass the guidance screens and directly select the SAL. The user may employ the General SAL guidance (consequence based) or the Federal Information Processing Standard (FIPS) 199 SAL guidance (based on FIPS 199 and National Institute of Standards and Technology (NIST), Special Publication (SP) 800-60).

The SAL value selected will limit the required questions to only those related to the selected level. The SAL value is also used in the ranking of missed questions.

For more information about Security Assurance Levels or SALs, see the [Security Assurance Level \(SAL\) Selection](#) help section.

### Standard Selection

Included on the Cybersecurity Standard Selection screen is a list of Standards and guides applicable to the mode options. The list of choices will vary depending on which mode is selected. Advanced users will have the option to select one or more Standards against which they would like to be evaluated.

For more information about Standards, see the [Standards Screen](#) help section.

## Assessment

### Questions

Once a Standard has been selected, CSET will generate a set of assessment questions that can be accessed from the Assessment screen. All questions will be answered as either Yes, No, Not Applicable (NA), or through an Alternate method (ALT). If the "Requirements" mode is selected, the questions will be presented as explicit requirements from the selected industry Standard.

The process of answering questions is tedious but straightforward. As a team, start with Question 1 and continue through each subject area or category until all questions have been discussed and answered.

### Mode Selection

There are two different methods to performing an assessment. The first uses a set of simplified Yes or No questions that have been extracted from industry Standards. These questions do not combine multiple concepts; rather, they address a single idea with each question.

The second mode presents the specific requirement text directly from the selected industry Standards. This requirement mode is designed for regulated industries where the exact wording

is important.

For more information, see [Mode Selection](#).

## **Results**

### **Dashboard**

The Results dashboard shows the basic score or results of the assessment at a glance. The overview shows 2 scores: (1) the overall score, and (2) a standards based score. It also shows charts for Assessment Compliance, Top Ranked Categories, Standards Summary, and Component Summary.

### **Analysis**

Assessment results can be reviewed in two locations. The first is from the Analysis Screen containing charts and tabular data that present both summary and detailed information about how well users are doing and where they need to improve, including rankings for questions by category and the questions themselves.

The second way to view assessment results is through a set of printed reports. From the executive to the site summary and the site detail reports, each report provides increasing levels of detail. Finally, the security plan report provides a template for documenting the required cybersecurity controls and the degree to which they are met. The printable reports contain charts, lists, and detail information found on the analysis screen.

For more information about Analysis, see the [Results](#) help section.

### **Reports**

The reports provide the details and scores of the assessment and allow for printing and publishing the assessment information, including summary charts and lists. Reports can help the user clearly understand where weaknesses are and where improvements should be made.

## **Additional Actions**

### **Utilize Assessment Documents**

CSET gives users the opportunity to collect and store all documents relevant to an assessment. This collection may be accomplished in two ways. First, all questions can have one or more documents associated with them indicated in the documents section of the details and resources link under each question. The second way is accessed from the Assessment Documents link accessed from the Help menu. The Document Library screen lists all documents currently associated with the assessment.

For more information, see the [Assessment Documents](#) help section.

### **Utilize Resource Library**

The Resource Library is a source for additional cybersecurity documentation. It is accessed from the [Title Bar](#) on the main CSET window. The Resource Library contains reference

materials to answer many technical or policy questions and aid in the creation and maintenance of a comprehensive cybersecurity program.

For more information, see the [Resource Library](#) help section.

## Protect Information

### Data Recovery

Unlike other versions of CSET, CSET 9.0 continuously saves data that is entered. If CSET is closed or the browser restarts all the entered data should remain.

## Disclaimer

The following disclaimer will be seen when installing CSET:

"The analysis, data, and reports in CSET® are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. In no event shall the United States Government or its contractors or subcontractors be liable for any damages, including but not limited to, direct, indirect, special, or consequential damages and including damages based on any negligence of the United States Government or its contractors or subcontractors, arising out of, resulting from, or in any way connected with this report, whether based on warranty, contract, tort, or otherwise, whether injury was sustained from, or arose out of the results of, or reliance upon the report."

"DHS does not endorse any commercial product or service, including the subject of the assessment or evaluation in this report. Any reference to specific commercial products, processes, or services by trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by DHS."

"The display of the DHS official seal or other DHS visual identities on this report shall not be interpreted to provide the recipient organization authorization to use the official seal, insignia or other visual identities of DHS. The DHS seal, insignia, or other visual identities shall not be used in any manner to imply endorsement of any commercial product or activity by DHS or the United States Government. Use of the DHS seal without proper authorization violates federal law (e.g., 18 U.S.C. §§ 506, 701, 1017) and is against DHS policies governing usage of the seal."

"The report is prepared and intended for internal use by the organization that made the request. The contents of this report may be subject to government or private intellectual property rights. To request distribution of this report outside the organization for which it was prepared, contact the CSET Program Office. The contents of this report may be reproduced or incorporated into other reports, but may not be modified without the prior express written permission of the CSET Program Office."

## System Basics

### System Requirements Local Installation

It is recommended that users meet the minimum system hardware and software requirements prior to installing CSET. This includes:

1. Pentium dual core 2.2 GHz processor (Intel x86 compatible)
2. 6 GB free disk space
3. 4 GB of RAM
4. Microsoft Windows 7 or higher.
5. Microsoft .NET Framework 4.6 Runtime. (included in CSET installation)
6. SQL Server 2012 Express LocalDB (included in CSET installation)
7. IIS Express 8.0 (included in CSET installation)

### System Requirements Enterprise Installation

It is recommended that users meet the minimum system hardware and software requirements prior to installing CSET. This includes:

- Pentium dual core 2.2 GHz processor (Intel x86 compatible)
- 8 GB free disk space
- 4 GB of RAM
- Microsoft Windows Server 2012 Edition or higher recommended
- Microsoft .NET Framework 4.6 Runtime
- SQL Server 2012 or higher recommended
- Internet Information Server (IIS)

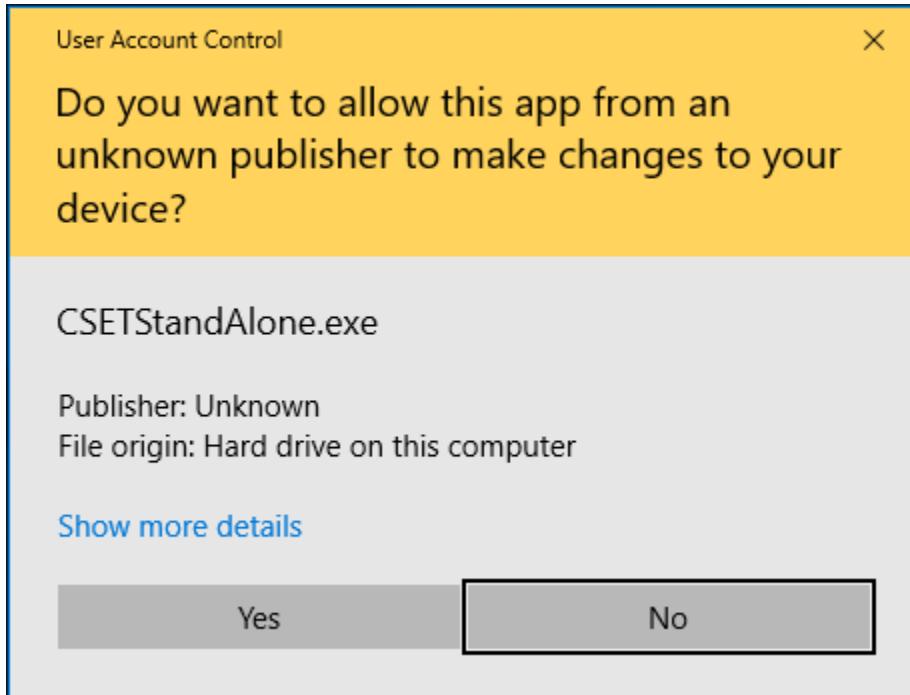
### Other Items of Note:

- For all platforms, it is recommended the user upgrade to the latest Windows Service Pack and install critical updates available from the Windows Update web site to ensure the best compatibility and security.
- If the install must be made through physical media, a USB port will be required.
- If desired, HTML reports will need to be converted to PDF using an external utility.
- If the Microsoft .NET Framework 4.6.0 Runtime is not available on the user's computer, CSET will automatically install it, which can add several minutes to the installation time. (For local installation)

# Installation Procedure

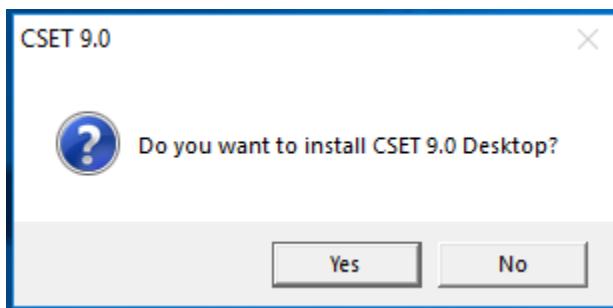
## Stand-alone Install

Double-click on the CSETStandAlone program.  
The User Account Control dialogue will come up. Select “Yes”.



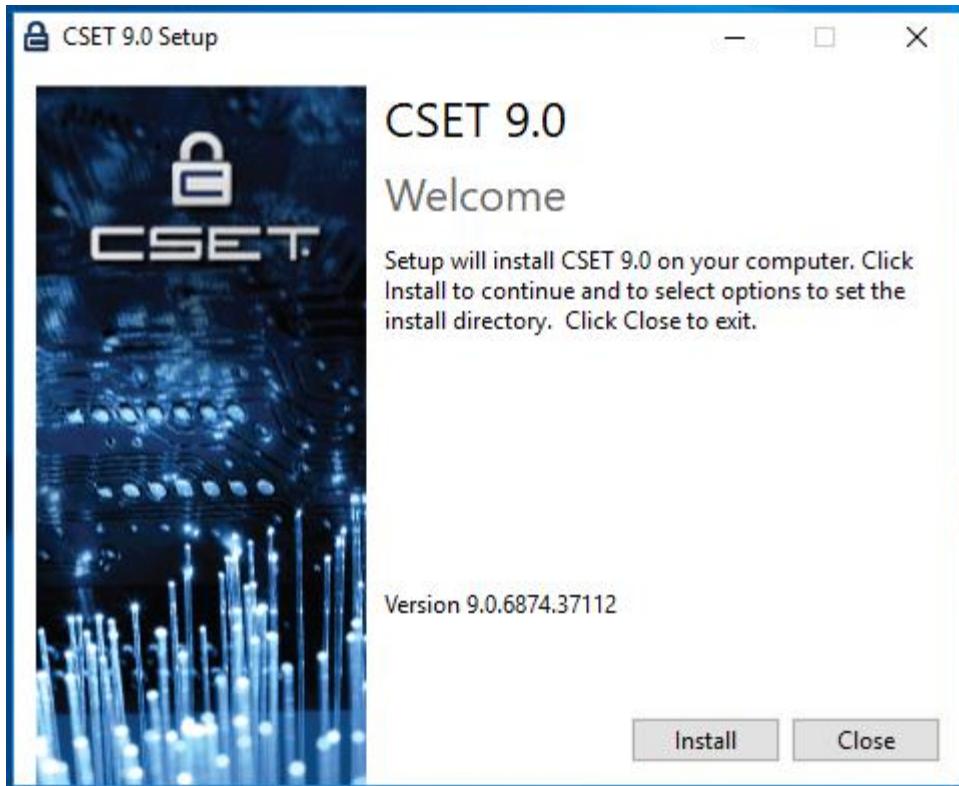
**Figure: User Account Control box**

A CSET 9.0 dialogue will open asking if you want to install CSET 9.0 Desktop. Select “Yes”.



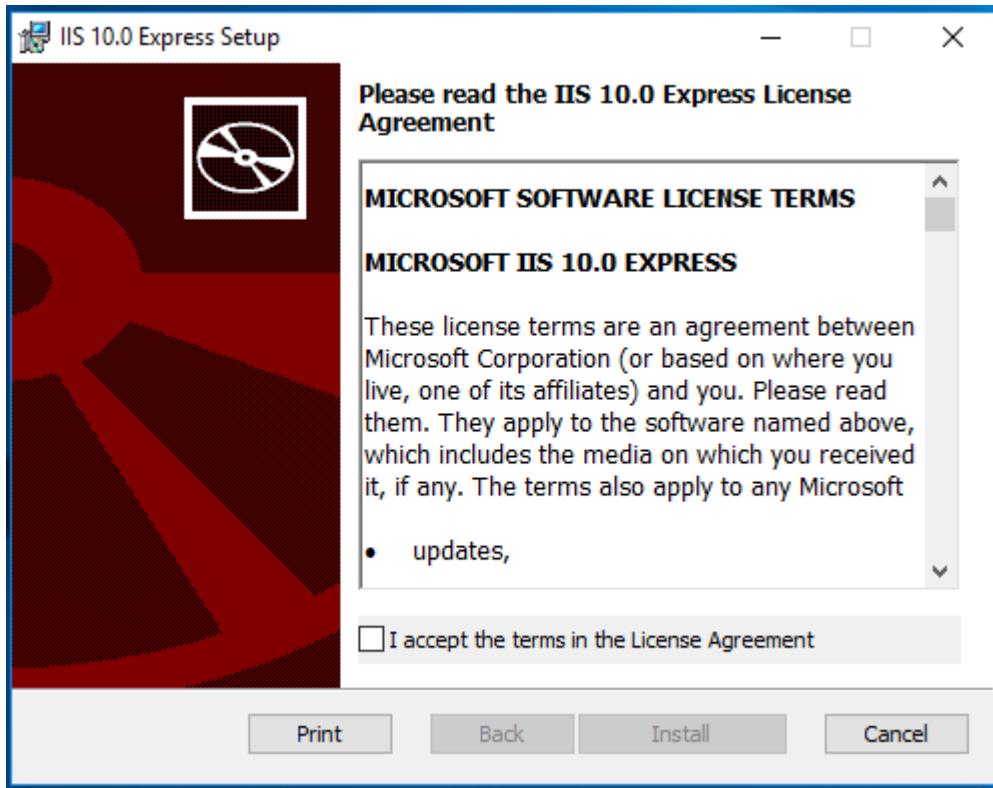
**Figure: Install dialogue**

The program will begin extracting.  
After extracting a CSET 9.0 Setup dialogue will open. Select “Install”.



**Figure: CSET Setup**

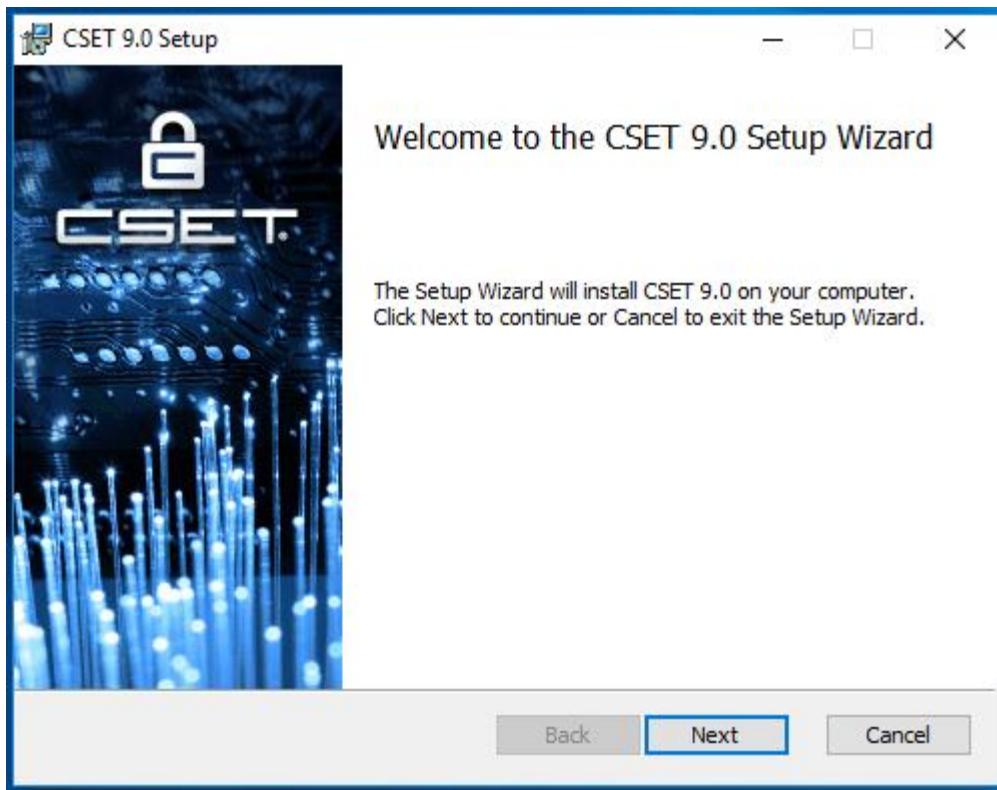
CSET will begin to install. If the user doesn't have IIS 10.0 Express, CSET will install it. The IIS 10.0 Express Setup dialogue will open. Click the check box to confirm that you "...accept the terms in the License Agreement", and then select "Install".



**Figure: IIS Setup**

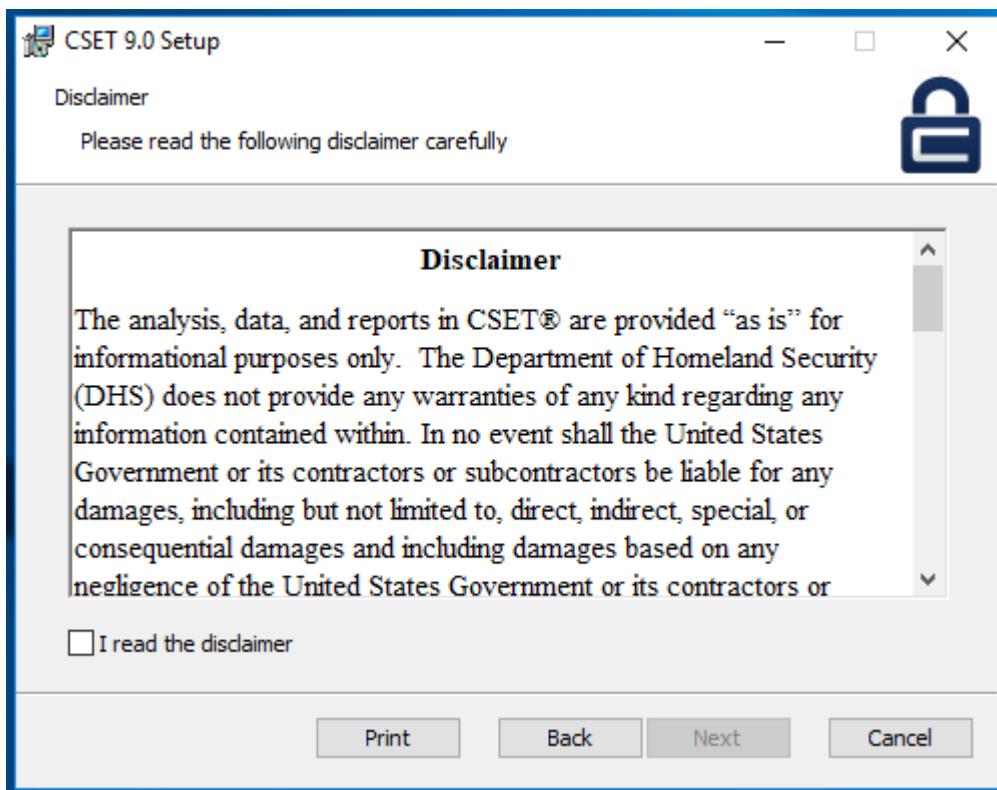
IIS will install. Select “Finish” when it completes.

The CSET 9.0 Setup Wizard will open to walk the user through the install process. Select “Next”.



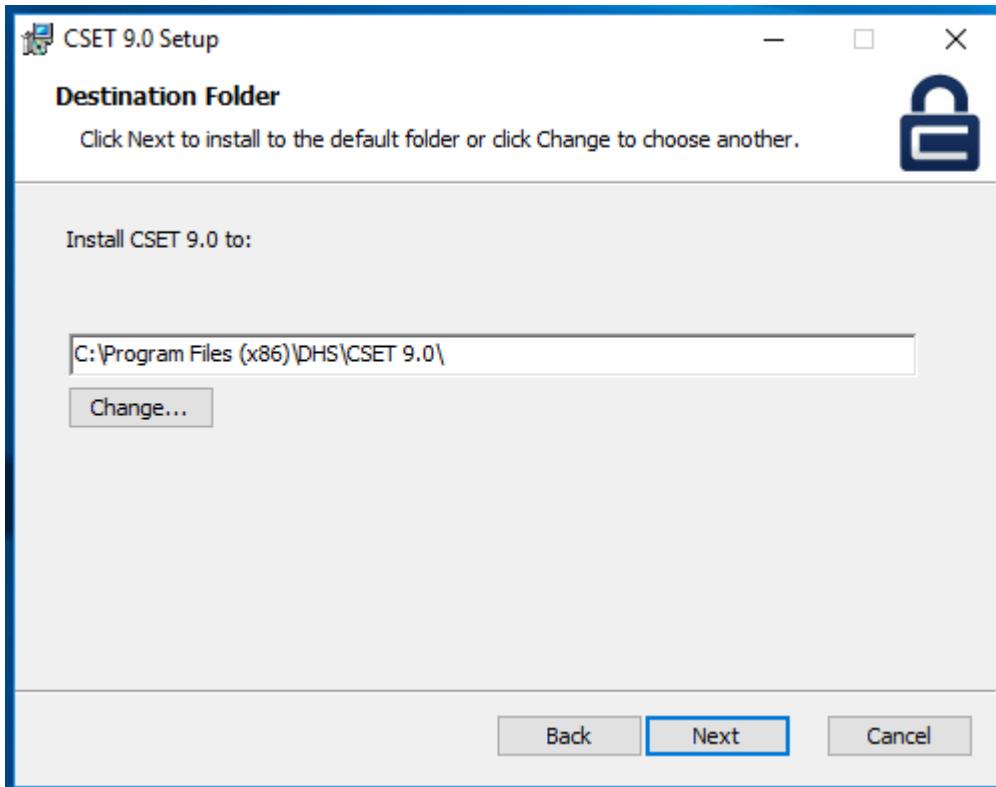
**Figure: Setup Wizard**

A disclaimer will open. Read through and then click the box “I read the disclaimer”, and select “next”.

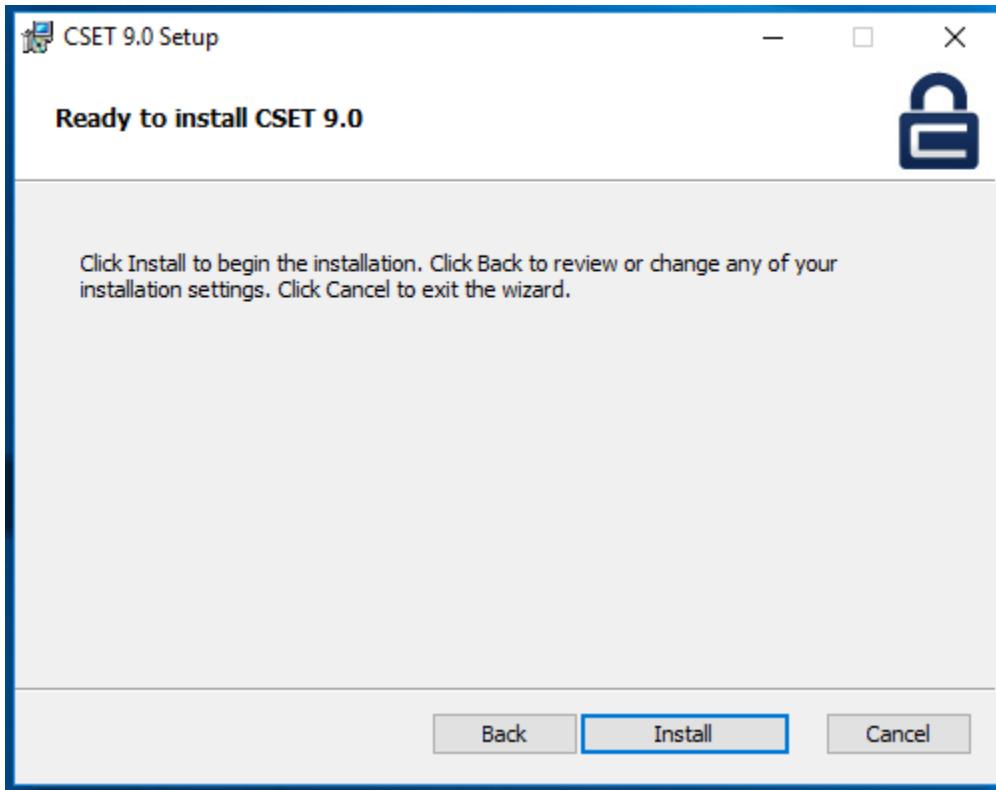


**Figure: Disclaimer**

CSET will choose a default folder to install CSET 9.0 to, but you can change this in the Destination Folder dialogue. Select “Next”.

**Figure: Destination Folder**

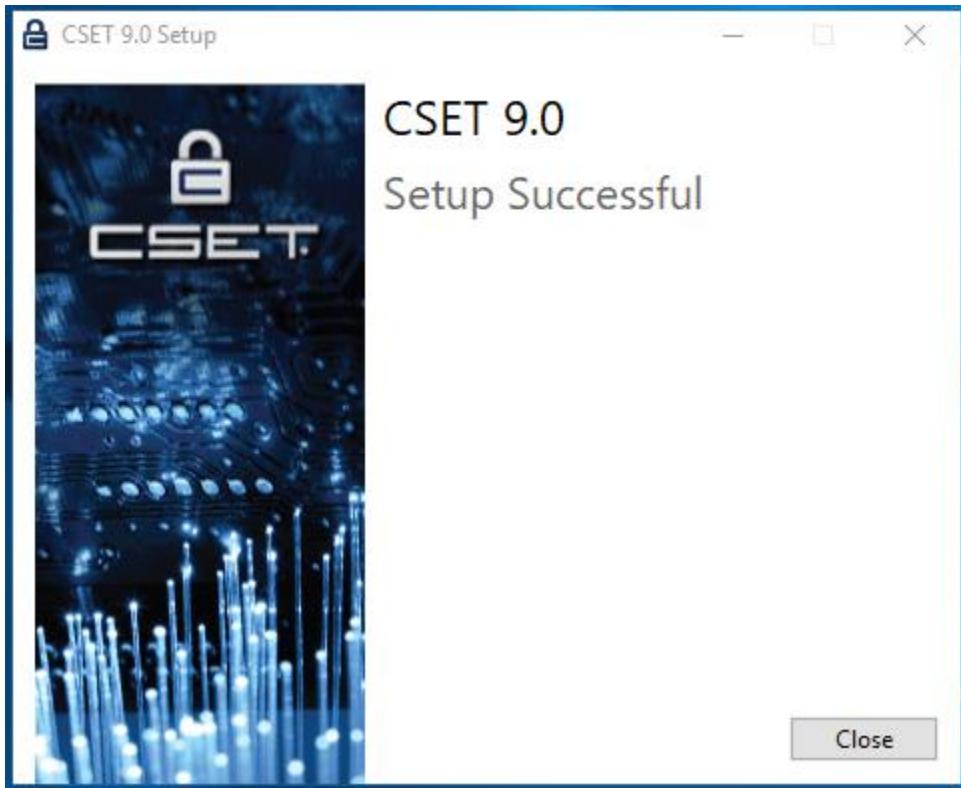
The CSET Installer will show that it is ready to install, select “Install”.



**Figure: Ready to Install**

CSET 9.0 will be installed. Make sure that the “Launch CSET 9.0 when setup exists” box is checked, and select “Finish”.

The user should see a setup successful dialogue, and then have an option of how they want to open the app. For this example, Edge was used.



**Figure: Setup Successful**

The user has access to CSET 9.0 as Local User. The Local Installation ribbon is visible at the top of the screen. They can see their landing page with no assessments at this time.

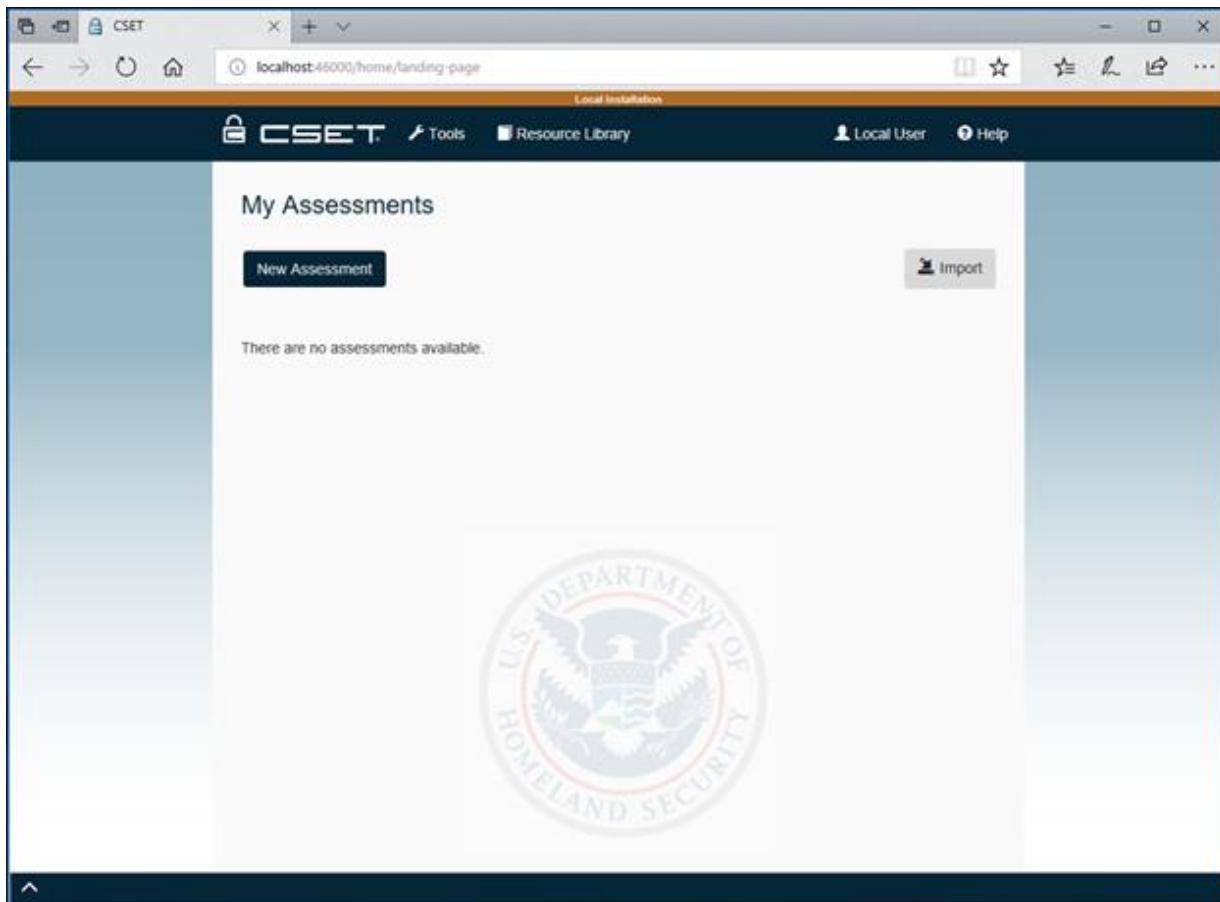


Figure: Local Install Landing Page

## Using the Stand-alone

There are a few things users should know in regards to the stand-alone install of CSET 9.0.

### Using the CSET System Tray Application

The CSET system tray app will be available in the user's task bar. To use it click the CSET icon .

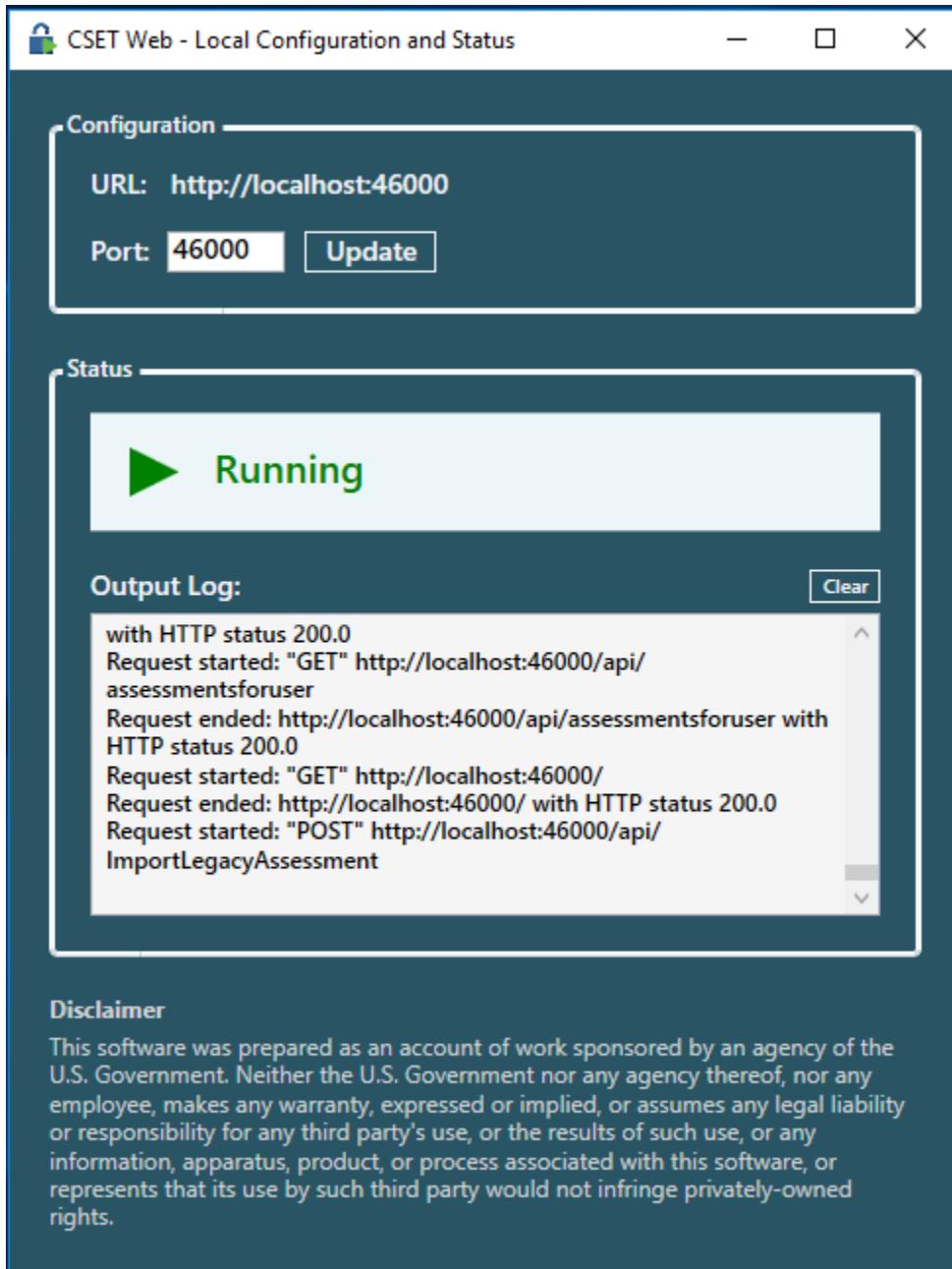
The user will have the option to Open CSET Web, Start CSET Web, Stop CSET Web, Configure/Status, or Exit.

Selecting "Open CSET Web" will open a web instance of CSET 9.0.

Selecting "Start CSET Web" will run the application. If the application is already running the Start CSET Web option will not be available, and the user should see in the Configure/Status that the Status is "Running".

Selecting "Stop CSET Web" will end the application.

Selecting "Configure/Status" will open the CSET Web- Local Configuration and Status box (Fig. #). The user can utilize this to change their port, check the status of the application, or check the output log.



**Figure: Local Configuration and Status box**

Selecting the "Exit" option will close the CSET system tray application menu.

# Enterprise Install

## Overview

This guide will detail the procedure for installing the latest version of the Cyber Security Evaluation Tool (CSET 9.0) in a web-based configuration on a Microsoft Windows Server 2016 instance running Microsoft SQL Server 2016.

## Prerequisites

In order to configure the CSET Database, an instance of Microsoft SQL Server Management Studio (SSMS) which is able to connect to the server instance will be required.

You will also need to obtain the latest CSET distribution. It can be downloaded from GitHub at <https://github.com/dhs-ncats/cset/archive/master.zip>. This file should be downloaded to the server or virtual machine, and should be extracted in a location where it will be accessible to the user.

NOTE: For the purposes of this document, a Windows Server 2016 instance, running inside a VMWare Workstation Pro 14 virtual machine will be used. The same VM will be running the database and the web server.

In order to host the database and web server on separate machines, the procedure given in this document will need to be modified accordingly, and extra care will be required in configuration steps (e.g.: the Web.config file will need to be edited to refer to the SQL Server machine, instead of localhost)

For other configurations, please refer to the applicable documentation from the relevant operating system and software vendors.

## Installation Steps

### IIS Setup

CSET is deployed as an IIS website. We will now install and configure the IIS Web Server for CSET deployment.

- Left click on "Add roles and features (button)" in "Server Manager"
- Select "Role-based or feature-based installation" and continue
- Select the "Web Server (IIS)" checkbox on the Server Roles list
- Expand the "Web Server (IIS)" list item, the "Web Server" list item, and the "Application Development" list item
- Select the ASP.NET 4.6 checkbox and continue
- Expand ".NET Framework 4.6 Features" list item on the Features list
- Select the "ASP.NET 4.6" checkbox and continue
- Select the "HTTP Redirection" checkbox in the Role Services list and continue
- Complete the installation

### SQL Server Installation

CSET requires a SQL Server database. In this document, we will install a new SQL Server instance on the Windows Server, and configure it for CSET. If a SQL Server instance already exists, skip this section, and continue to Additional Dependencies. Ensure you have administrative access and privileges on the database.

- Insert the SQL Server disk, or mount the disk image and run Setup.exe
- Click the “Installation” link on the navigation pane on the left
- Click the “New SQL Server stand-alone installation or add features to an existing installation” link
- Enter your product key and continue, accepting the license terms
- At the Feature Selection screen, select the “Database Engine Services” checkbox on the Features list and continue
- At the Database Engine Configuration screen, select the “Mixed Mode (SQL Server authentication and Windows authentication)” radio button
- Enter (and confirm) a password for the server administrator (sa) account
  - Take note of this password. It will be required in a later step
- Click the “Add Current User” button and continue when the user information appears in the text box
  - It may take a few moments for the user information to appear in the text box
- Complete the installation

## Additional Dependencies

There is some additional software required by CSET. We will now install this software. The software required is the Microsoft URL Rewrite Module 2.0 for IIS. It can be obtained through the Microsoft website at <https://www.microsoft.com/en-us/download/details.aspx?id=7435>. Simply download the file to the server and run it. This will install the module needed for IIS to function properly with CSET.

## Firewall Configuration

In order to configure and use the new SQL Server instance, it needs to be able to receive incoming connections. By default, this is prevented by the Windows firewall. We will now reconfigure the firewall to allow incoming database connections.

- From the Windows “Start” menu, search for “firewall”, and select “Windows Firewall with Advanced Security”
- On the navigation pane on the left, click “Inbound Rules”
- On the Actions pane on the right, click “New Rule...”
- Select the “Port” radio button and continue
- Select the “Specific local ports” radio button
- In the text field, input **1433** and continue
- Select the “Allow the connection” radio button and continue
- On the Profile screen, select which networks you wish to allow incoming connections from, and continue
- Enter a name and a description for this rule, and continue

- oThe description is optional, but the name should reference SQL Server

## Database Setup

The database used by CSET must be configured properly for CSET. This step involves configuring the SQL Server instance installed in a previous step.

- On the server or virtual machine, navigate to the CSET Distribution which was downloaded previously
- In the “Database Images” folder, there are two files: CSETWeb.mdf and CSETWeb\_log.ldf.
- Copy these files to a suitable shared location such as the root of the C: drive
  - oYou will need to ensure that users have adequate permissions to read and modify both files
- On a host or client machine, open SSMS
- Connect to the SQL Server instance using an administrative account, such as the ‘sa’ account created while installing the SQL Server instance in the previous step
  - oThe server or virtual machine needs to be configured to be reachable on the network by the host or client machine, but this is outside of the scope of this document
- In the navigation pane on the left, right click on Databases
- Click Attach
- In the Attach Databases dialog, click the Add button
- In the Locate Database Files dialog, navigate to the folder you copied the database images to
- Select CSETWeb.mdf and click OK
- In the Attach Databases dialog, click OK
- In the navigation pane on the left, under Databases, CSETWeb should appear

## CSET Installation

With the system properly configured, CSET itself can now be installed.

- On the server or virtual machine, navigate to the CSET Distribution which was downloaded previously
- Navigate to the ‘dist’ folder
  - oThe contents of this file will need to be copied to the folder for the IIS website it is being deployed to
- In the navigation pane on the left side of the Server Manager window, click IIS
- In the SERVERS list, right click on the server instance you will be deploying to
  - oIf you have followed the installation instructions given, it will be the only item in the list, and will be highlighted
- Click “Internet Information Services (IIS) Manager” on the right-click menu
- In the “Internet Information Services (IIS) Manager” window, on the left navigation pane, locate the server name, and expand that list item
- Expand the Sites list item
- Click on the “Default Web Site” list item
- In the Actions pane on the right side, click Explore
- A new Windows Explorer window will appear
- Remove the files in that folder, **but do not delete the ‘aspnet\_client’ folder**
- Copy all of the contents of the ‘dist’ folder (inside the CSET distribution) into this folder

## CSET Configuration

Now that CSET is installed, it must be configured before it can be used.

- In the website folder found in the “CSET Installation” steps, locate the file Web.config
- Open this file in a text editor such as Notepad
  - You will need to ensure you have proper permissions to modify this file before editing
- Locate the section of code between the `<connectionStrings>` and the `</connectionStrings>` tags
- On each of these lines, locate the words *data source*
- Edit these to reference the IP address or domain name of the machine that the SQL Server instance is installed on (e.g.: `data source=domain.name.here` or `data source=123.456.789.012`)
  - If IIS and SQL Server are running on the same machine, then use `localhost` as the domain name
- Edit the lines to indicate login credentials after `persist security info=True;`
  - If SQL Server authentication will be used, then a user id and password will need to be provided for the login that will be used
    - E.g.: `user id=cset_user;password=AbC!2#;`
    - If Windows domain authentication will be used, then the user id and password will need to be replaced with `Trusted_Connection=True;`

## Evaluation Preparation

Two preliminary tasks are required before using the tool to perform an assessment: (1) forming the subject matter team and (2) collecting the network/architecture documentation and related information.

### Subject Matter Team Selection

The first step is to select a cross-functional assessment team consisting of subject matter experts selected from various operational areas in the organization. Organizations may add additional team members as needed to address specific topics. Anyone in the organization who has had training or experience with the CSET tool should be included on the team.

The primary user should spend some time using the CSET tool with test-only or dummy data prior to commencement of the team activity. Familiarity with the CSET tool will improve speed and ease of use.

Representatives from the following areas are suggested for an effective assessment. The representatives should have significant expertise in their areas of responsibility.

If performing an ICS assessment:

- Industrial Control Systems (knowledge of industrial control system architecture and operations)
- System Configuration (knowledge of systems management).
- System Operations (knowledge of system operation).

For either an ICS or IT assessment:

- IT Network/Topology (knowledge of IT infrastructure).
- IT Security/Control System Security (knowledge of policies, procedures, and technical implementation).
- Risk Management (knowledge of the organization's risk management processes and procedures).
- Business (knowledge of budgetary issues and insurance postures).
- Management (a senior executive sponsor/decision maker).

### Gather Supporting Documentation and Information

Previous CSET users have found that the following types of documents and information are useful to have during completion of the assessment. Collecting this reference information before beginning the assessment is advisable:

- Organizational chart that outlines responsibilities;
- Annual operating and capital budgets;
- Insurance policy description;
- Previously performed risk and vulnerability assessments;
- Capacity, operation, management, and maintenance manuals;
- Risk management documentation;
- Hazardous waste operations and emergency response Standards;

- Emergency Operations Plan/Emergency Response Plan;
- Asset inventory and criticality rating from Computerized Maintenance Management System (CMMS);
- Inventory list of process control/SCADA software and hardware, including interfaces;
- Network topology diagram and supporting documentation;
- Documentation/knowledge from previous incidents or near misses;
- General asset inventory, criticality asset determination, business impact analyses, contingency plans, etc.; and
- Information security policies, plans, and procedures.

When the assessment team is prepared and supporting documents are gathered, the organization is prepared to start CSET and begin the actual evaluation.

## Start CSET

Go to <http://localhost:46000/index.html> or for other installation options the instructions provided in the help section titled [Installation Procedure](#) should be followed.

The actual URL maybe provided by your companies CSET administrator.

The CSET Home Screen will be displayed as seen in the Figure below.

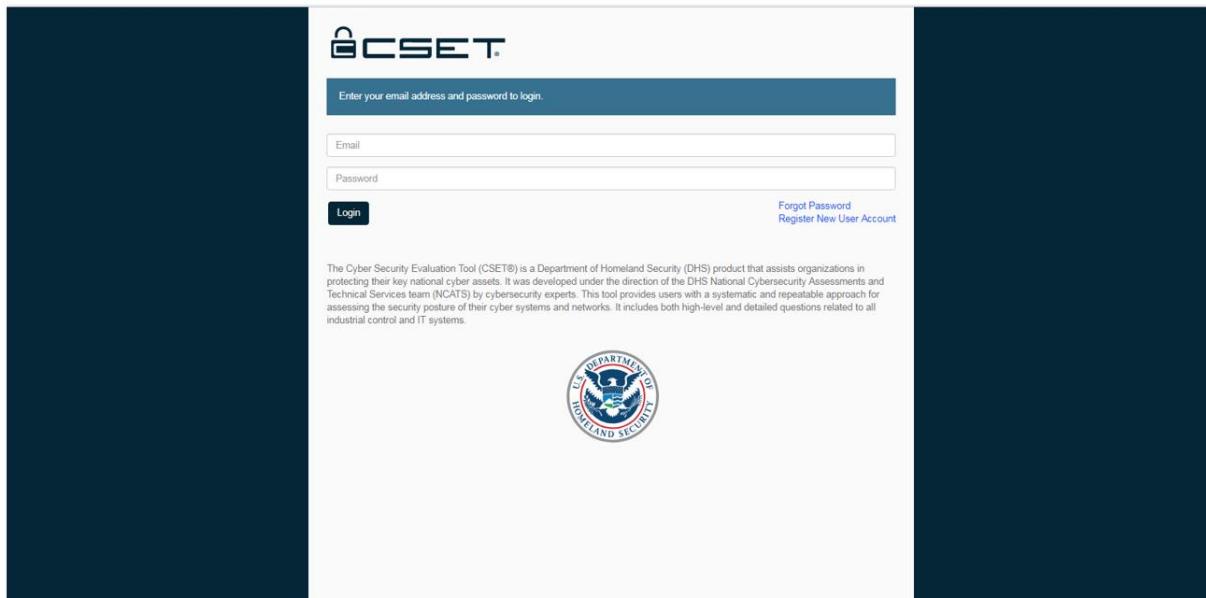


Figure: CSET Home Screen

# Register a User Account

To get started in CSET you must have a registered account. This is an easy process that won't take much time at all.

First, select the "Register New User Account" link. The Register Account dialogue will open.



Figure: Using the Home page to register an account



Enter your name and email address to register.

First Name \*

Last Name \*

Email \*

Confirm Email \*

**Register**

Registered User Login

**Figure: Registration dialogue**

The user should enter in their first and last name and email. Then select the "Register" button. The user will be sent an email with a temporary password and instructions to login. Users can navigate to CSET through the email or select the "Registered User Login" link on the dialogue above.

Warning: Users CAN NOT register an email that has already been registered.

1

## Register Account link

[Register New User Account](#)

This link will open a dialogue for the user to create a new account.

2

## Forgot Password link

[Forgot Password](#)

This link opens a dialogue for user's to get a new temporary password and reset their old forgotten password.

3

## Login Email and Password fields

Email

Password

To login enter the user's email and password here.

4

## Login button

[Login](#)

Click the login button after entering user information to login.

## Import/Export a CSET Assessment

### Importing a .csetw File

With a web-instance of CSET 9.0 a user can import a .csetw file. To begin click the Import button to begin the process.



**Figure: Import Button**

The user's File Explorer will open, and at this point they can select a .csetw file. A new assessment that is a duplicate of the uploaded assessment will show in the user's landing page.

NOTE: The web-instance of CSET 9.0 only supports .csetw file upload. For legacy file (.cset) upload the user must use the stand-alone install.

## Importing a .cset File

With the Stand-alone version of CSET 9.0 running locally the user can import a legacy CSET file.



Much like importing a .csetw file click the button on the local Landing page.

The user's file explorer will open. Select the .cset file to import. The upload dialogue will open. Once the dialogue has closed, refresh the Landing page to see the imported assessment.

## Exporting a CSET Assessment

To export an assessment simply select the Export button next to the assessment to be exported on the Landing page.



**Figure: Export button**

After clicking the Export button the assessment will be downloaded as a .csetw file and will be in the user's Downloads folder (unless otherwise specified in browser settings).

## Custom Questionnaires

The Custom Questionnaire Manager allows the user to define custom subsets of questions or requirements for an assessment. Questions may be selected from any Cybersecurity Standard currently used and defined in the CSET tool. The following sections describe how to create and work with Custom Questionnaires.

## Using the Import New Module

NOTE: The Import New Module is designed for Developer use. The user needs experience with either JSON or XML. To access the Import New Module visit  
[www.csetac.inl.gov/importmodule](http://www.csetac.inl.gov/importmodule)

There are a few different options to import a new Questions or Requirements set in CSET 9.0. The user can use an edit an existing standard, create their own JSON or XML module in CSET, or use a schema in an outside code editor and paste in CSET.

The parts of the Import New Module can be seen in the Figure below.

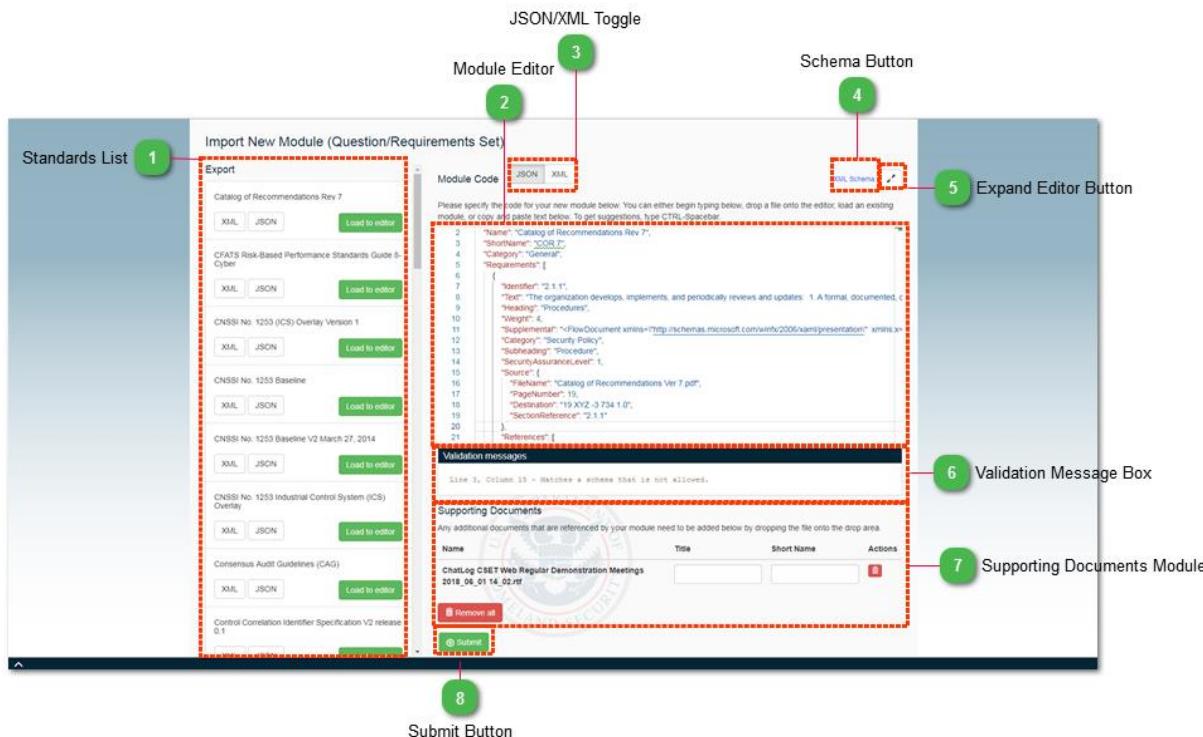


Figure: Import New Module screen

1

### Standards List

The Standards List displays a list of cybersecurity standards:

- Catalog of Recommendations Rev 7
- CFATS Risk-Based Performance Standards Guide 6-Cyber
- CNSSI No. 1253 (ICS) Overlay Version 1
- CNSSI No. 1253 Baseline
- CNSSI No. 1253 Baseline V2 March 27, 2014
- CNSSI No. 1253 Industrial Control System (ICS) Overlay
- Consensus Audit Guidelines (CAG)
- Control Correlation Identifier Specification V2 release 0.1

Each standard entry includes XML and JSON export buttons and a "Load to editor" button.

The Standards List allows the user to export any of the standard code in either XML or JSON. It also allows the user to click "Load to editor" to load any standard code to the Module Editor where it can be edited. When a new standard is imported it will show in the Standard List, as well as, the Cybersecurity Standards page.

2

## Module Editor

```

2   "Name": "Catalog of Recommendations Rev 7",
3   "ShortName": "COR 7",
4   "Category": "General",
5   "Requirements": [
6     {
7       "Identifier": "2.1.1",
8       "Text": "The organization develops, implements, and periodically reviews and updates: 1. A formal, documented, c
9       "Heading": "Procedures",
10      "Weight": 4,
11      "Supplemental": "<FlowDocument xmlns='http://schemas.microsoft.com/winfx/2006/xaml/presentation'><xmlins.x<
12      "Category": "Security Policy",
13      "Subheading": "Procedure",
14      "SecurityAssuranceLevel": 1,
15      "Source": [
16        {
17          "FileName": "Catalog of Recommendations Ver 7.pdf",
18          "PageNumber": 19,
19          "Destination": "19 XYZ -3 734 1.0",
20          "SectionReference": "2.1.1"
21        }
22      ],
23      "References": []
24    }
25  ]

```

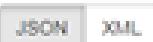
The Module Editor is where the user can edit or create a new standard for import. Edit within the tool or drag and drop a file to the editor.

Tip: Use CTRL+Spacebar to see list options while coding. Use ALT+Shift+F to format code when loaded from the Standards List.

Note: New Standards can contain both Questions and Requirements. If only using Requirements they will be duplicated for the Questions set.  
Short Names must be unique when editing a previously used standard.

3

## JSON/XML Toggle



Use the JSON/XML Toggle to pick what language to use for the new standard being imported. It is recommended to use JSON, because CSET has more comprehensive validation and list options within the editor.

4

## Schema Button



Use the Schema button to download a code schema to edit in an outside editor. Drag and drop the file when complete to see validation messages and submit.

5

## Expand Editor Button



Click the Expand button to expand the Module Editor to the full-screen.

6

## Validation Message Box



The Validation Message box shows errors in the code, as well as, processing errors when a user hits "Submit".

7

## Supporting Documents Module

A screenshot of the Supporting Documents Module. At the top, it says "Supporting Documents". Below that, there's a note: "Any additional documents that are referenced by your module need to be added below by dropping the file onto the drop area." A table follows, with columns: Name, Title, Short Name, and Actions. There is one row in the table with the following data:  
Name: ChatLog CSET Web Regular Demonstration Meetings  
Title: 2018\_06\_01\_14\_02.ref  
Short Name: (empty)  
Actions: A red trash icon.  
At the bottom left, there's a red button labeled "Remove all".

Users can add supporting documents and references with the newly created standard. Drop reference files into the reference file drop area, enter a title, and a short name. Use the red trash icon or remove all to delete supporting documents.

Tip: If using the Destinations field in the editor to direct a user to a certain place in the supporting document, then the destinations must be set up in the support document itself. See [Choose Your Destination](#) for more information.

8

## Submit Button



Select "Submit" when the module code is complete and ready to be created.

## Title Bar

The Title Bar allows the user to access high-level functions of the CSET application and is shown in the Figure below.

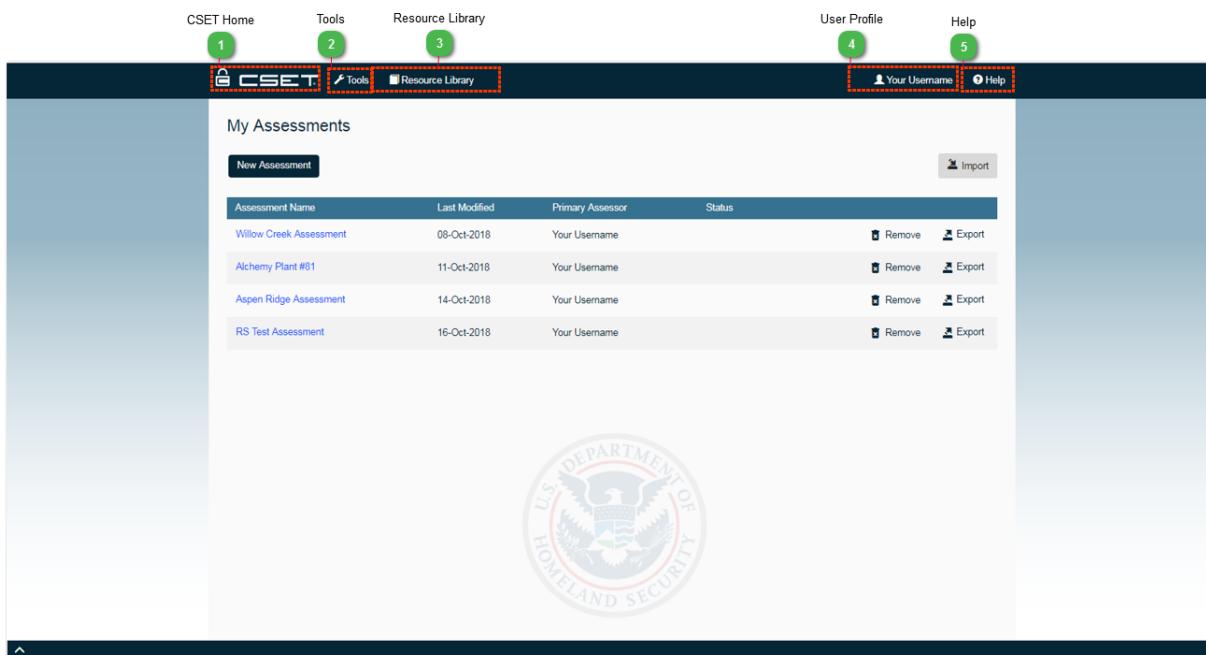


Figure: Title Bar

1

### CSET Home



The CSET HOME button opens the user's landing page.

For more information about the landing page, see the [Landing Page](#) help section.

2

### Tools



The Tools button opens the Tools menu.

For more information about the Tools menu, see the [Tools Menu](#) help section.

3

### Resource Library



The Resource Library button opens the Resource Library.

For more information about the Tools menu, see the [Resource Library](#) help section.

4

## User Profile



(This will display your user name)

The User Profile button opens the User Profile menu.

For more information about the User Profile menu, see the [User Profile](#) help section.

5

## Help

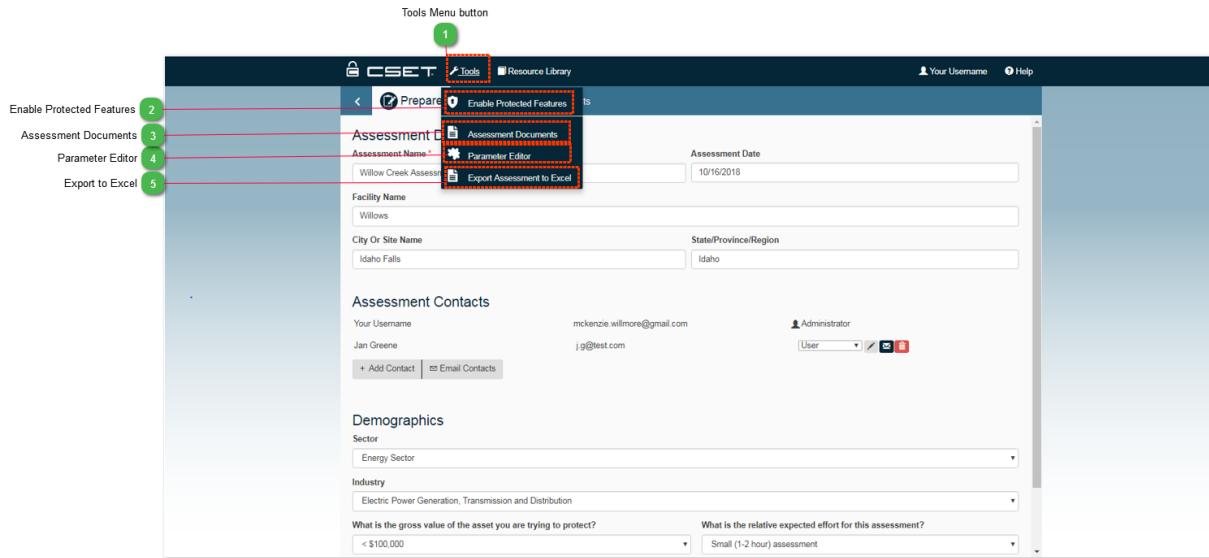


The Help button opens the Help menu.

For more information about the Help menu, see the [Help Menu](#) section.

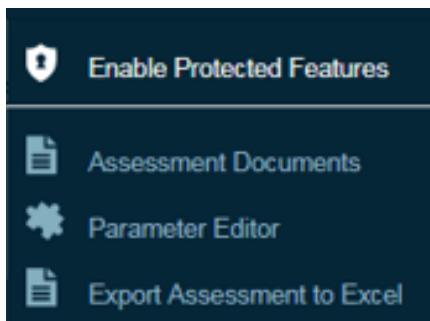
## Tools Menu

The Tools Menu provides the user with options outside of the assessment process. The user can access the Enable Protected Features, Assessment Documents, Parameter Editor, and Export Assessment to Excel features. The Tools Menu is described in the Figure below.



**Figure: Tools Menu**

NOTE: The Assessment Documents, Parameter Editor, and Export to Excel features are not available unless within an assessment. If on the landing page the Tools menu will look like the Figure below.



**Figure: Tools menu outside of an assessment**

1

### Tools Menu button



Clicking the Tools menu button opens up the Tools menu.

2

## Enable Protected Features



Clicking the Enable Protected Features menu item displays the Protected Features window that allows the user to view specific questionnaires or standards developed by specific industries that are not available to the general public.

See [Protected Features](#) for more information.

3

## Assessment Documents



Clicking the Assessment Documents menu item opens the Assessment Documents window that allows users to review documents that have been assigned to specific questions of the assessment. If there are no documents associated with the assessment the list will return blank.

See [Assessment Documents](#) for more information.

4

## Parameter Editor



Clicking the Parameter Editor menu item displays the Parameter Editor window where users can maintain parameters related to their selected Standard in requirements mode, if they are supported.

See [Parameter Editor](#) for more information.

5

## Export to Excel



Clicking the Export to Excel menu item downloads an excel spreadsheet with the answers to the assessment Questions or Requirements.

See [Export to Excel](#) for more information.

## Assessment Documents

This section contains information on the purpose and use of CSET Assessment Documents. The Assessment Documents window stores documents and files added to the assessment by the user. These files are associated with specific questions to help explain or to provide evidence for the answer given.

The assessment documents window provides a way to see all the files that have been stored in the assessment by the user. During the assessment, a document can be added using the Add Document button in the documents section of the Question Details panel that will associate the document with that question. The Assessment Documents is accessed from the Tools menu.

The [Documents](#) help section provides more detailed information on how to associate documents with a question.

Clicking the Assessment Documents menu item in the Tools Menu displays the Assessment Documents window seen in the Figure below.

View or download assessment documents via the dialogue.



Figure: Assessment Documents Window

## Parameter Editor

Many Cybersecurity Standards in CSET contain parameter information in the requirement text. Parameters are indicated by [] symbols in the requirement text. For example, the SP800-53 R4 App J Standard contains the following parameter: [Assignment: organization-defined frequency, at least annually].

The Default Parameter Editor allows the user to replace the default parameter text with other text the user defines. So in the previous example, the user might replace the [Assignment: organization-defined frequency, at least annually] parameter with the word Annually. The Default Parameter Editor will then replace all occurrences of the parameter with the user's text.

Users can also change the parameters within the Requirement text itself with inline parameter editing. Simply click in to the parameter edit and save.

The Default Parameter Editor window is described in the Figure below.

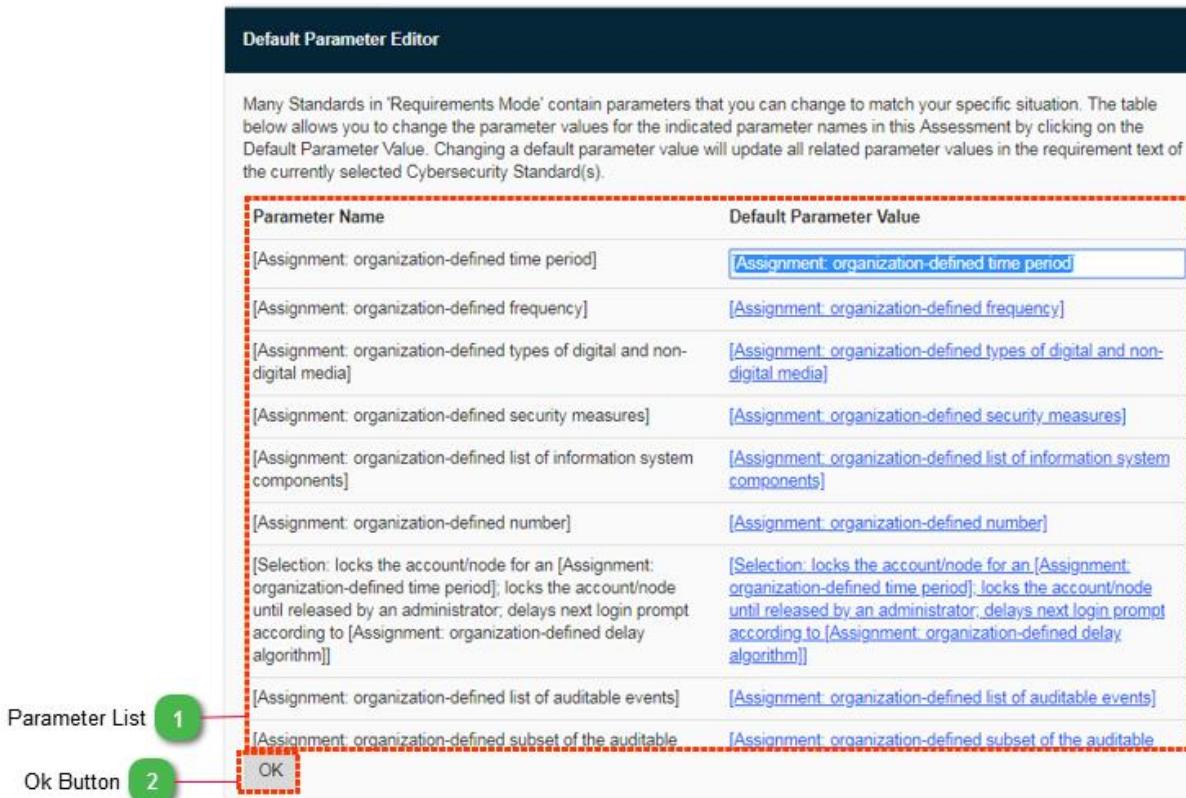
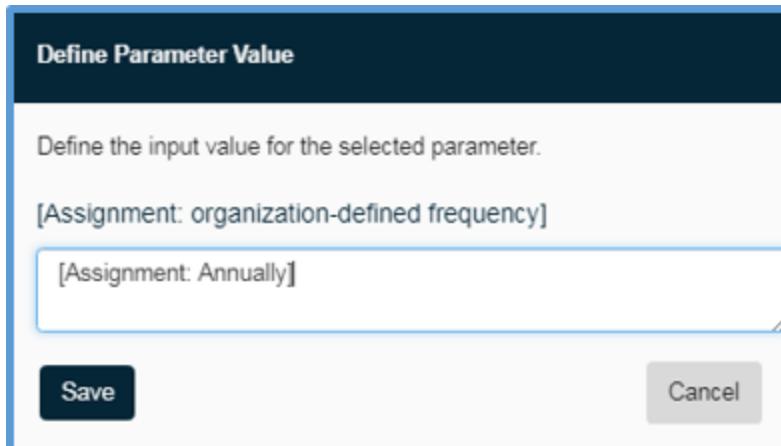


Figure: Default Parameter Editor Window



**Figure: Inline Parameter Editing**

1

## Parameter List

Parameter Name	Default Parameter Value
[Assignment: organization-defined time period]	[Assignment: organization-defined time period]
[Assignment: organization-defined frequency]	[Assignment: organization-defined frequency]
[Assignment: organization-defined types of digital and non-digital media]	[Assignment: organization-defined types of digital and non-digital media]
[Assignment: organization-defined security measures]	[Assignment: organization-defined security measures]
[Assignment: organization-defined list of information system components]	[Assignment: organization-defined list of information system components]
[Assignment: organization-defined number]	[Assignment: organization-defined number]
[Selection: locks the account/node for an [Assignment: organization-defined time period]; locks the account/node until released by an administrator; delays next login prompt according to [Assignment: organization-defined delay algorithm]]	[Selection: locks the account/node for an [Assignment: organization-defined time period]; locks the account/node until released by an administrator; delays next login prompt according to [Assignment: organization-defined delay algorithm]]
[Assignment: organization-defined list of auditable events]	[Assignment: organization-defined list of auditable events]
[Assignment: organization-defined subset of the auditable	[Assignment: organization-defined subset of the auditable

The Parameter List displays a list of Parameter Names and associated Default Parameter Values.

The Parameter Name column shows the name of the parameter and cannot be changed.

The Default Parameter Value column displays the current parameter values associated with the parameter names for the selected Standards as seen in the Requirement text on the Assessment screen. The parameter values are initially the same as the Parameter Name but can be changed by the user. To change a parameter value,

double-click the cell containing the desired Default Parameter Value and enter new parameter text. Perform the same with any other parameters. Once finished, click the "Ok" button.

All parameter values in the requirement text will then be updated with the entered text for the given parameter names throughout the assessment.

2

## Ok Button

OK

The Ok closes the Default Parameter Editor and updates any relevant blue parameter links in the Question Content Area with changes to the parameter values.

## Protected Features

The Protected Features window allows the user to add a feature unlock code to release specific standards or questionnaires that are not available to the general public. The Protected Features window is described in the Figure below.

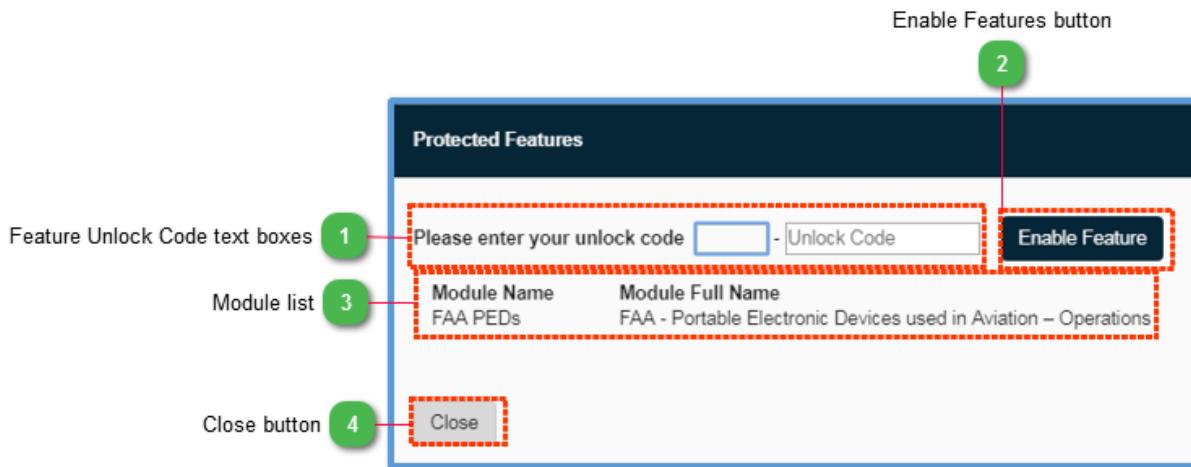


Figure: Protected Features Window

1

### Feature Unlock Code text boxes

Please enter your unlock code  -

The Feature Unlock Code input text boxes allow the user to enter the feature unlock code. Once a proper code has been entered, the Module List will display all available standards or questionnaires that can be added to the CSET Standards Selection screen.

2

### Enable Features button

Select the Enable Feature button after entering the Unlock Code.

3

### Module list

Module Name	Module Full Name
FAA PEDs	FAA - Portable Electronic Devices used in Aviation – Operations

The Module List displays a list of available standards or questionnaire modules that are unlocked and available in the Cybersecurity Standards Selection page.

4

## Close button

A small, light gray rectangular button with a thin black border and the word "Close" centered inside in a small, black, sans-serif font.

The Close button closes the Protected Features dialogue and commits changes.

## Export to Excel

Selecting the "Export to Excel" link will download an excel copy of your assessment results.

NOTE: The excel report shows either Questions or Requirements. Whichever mode has more answers will show in the report.

A	B	C	D	E	F	G	H	I	J	K	L	M	N
Question_Id	Question_Group_Heading	Simple_Question	Answer_Text	Mark_For_Review	Is_Question	Is_Requirement	Is_Component	Is_Framework	Component_Id	Answer_Id	Comment	Alternate_Justification	Compc
1	6223 Policies Procedures General	The facility should have documented and distributed: 1. Cyber security policies (including a change management policy). 2. Plans/processes and supporting procedures commensurate with the facility's current IT operating environment.											
2	6224 Policies Procedures General	The facility should designate one or more individuals to manage cyber security who can demonstrate proficiency through a combination of training, education, and/or experience sufficient to develop cyber security policies and procedures and ensure compliance with all applicable industry and governmental cyber security requirements.	Y	False	False	True	False	False	0	38360			
3	6225 Access Control	The facility should identify and document systems boundaries (i.e., the electronic perimeter) and has implemented security controls to limit access across those boundaries.	Y	False	False	True	False	False	0	38361			
4	6226 Access Control	The facility should establish and document a business requirement for every external connection to/from its critical systems. The facility external connections should have controls that permit access only to authorized and authenticated users.	N	False	False	True	False	False	0	38362			
5	6227 Access Control	The facility should practice the concept of least privilege.	NA	False	False	True	False	False	0	38363			
6			A	False	False	True	False	False	0	38364			

**Figure: Export to Excel Output**

## Resource Library

The Resource Library is an excellent way to help the user better understand and resolve the concerns identified by the assessment and to improve the security of the user's systems. It contains a variety of Standards, reports, templates, white papers, plans, and other cybersecurity-related documents. The Figure below shows the Resource Library window.

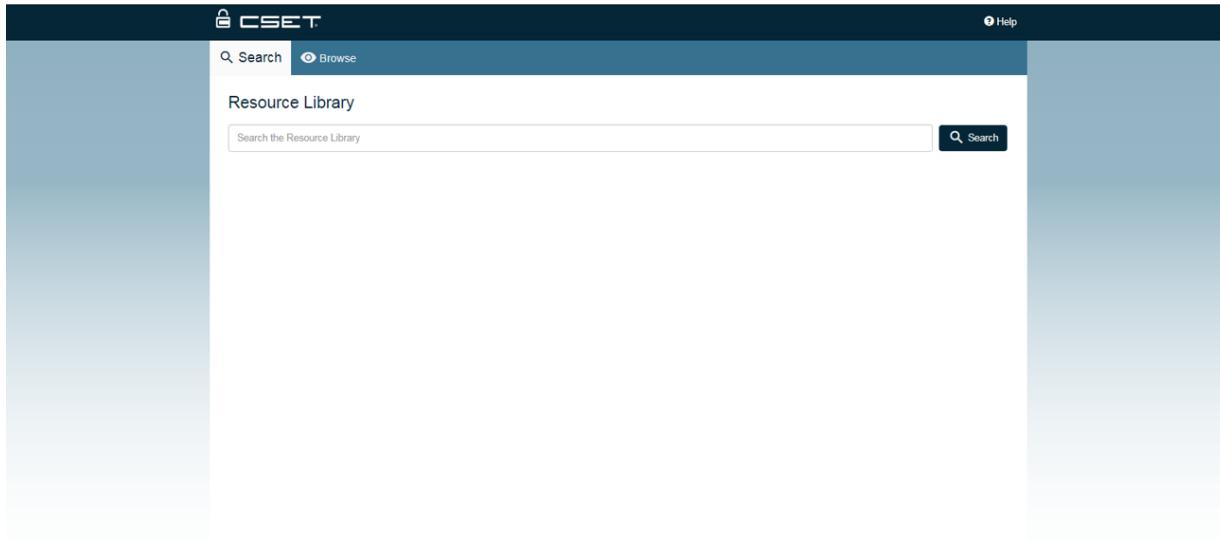


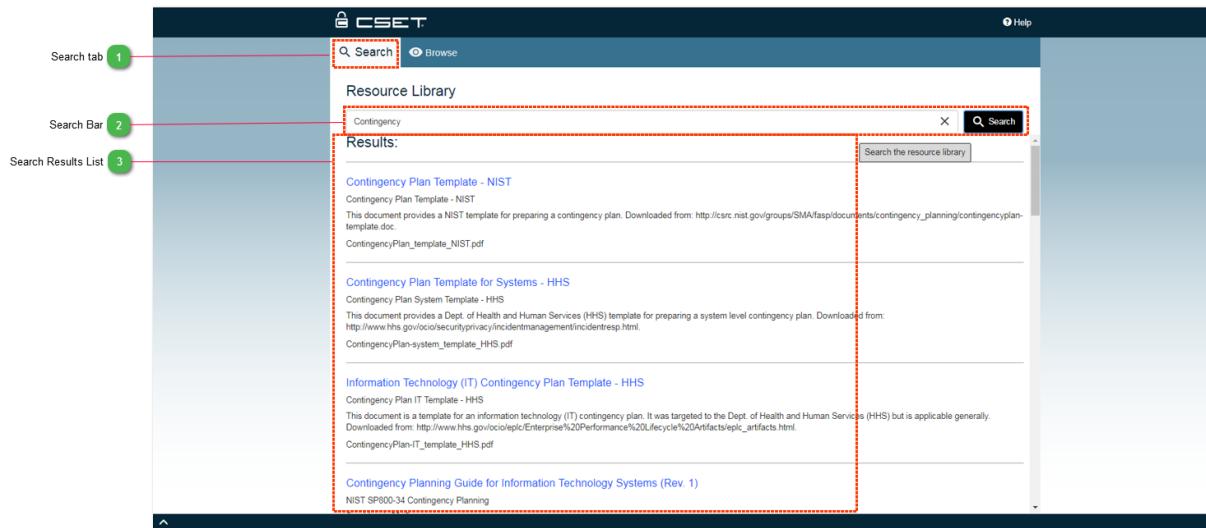
Figure: Resource Library Window

## Search Screen

Two ways are available to find documents within the Resource Library. This section discusses the Search feature. The other way is by using the document tree structure discussed in the help section titled [Browse Screen](#).

The Search screen option of the Resource Library provides a way to find a list of documents based on the text string typed into the search box. Clicking the Search tab opens a search box. Enter the desired text string and click on the magnifying glass icon or press the keyboard Enter key to begin the search.

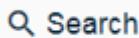
The Figure below shows an example where the user has typed in the string "contingency." In this case, CSET searches through all the documents for occurrences of the word "contingency" and then ranks and presents them in an ordered list in the Search Results.



**Figure: Resource Library Search Screen**

1

### Search tab



Clicking the Search tab will display the search functions of the Resource Library. The Resource Library always opens to the Search tab.

2

### Search Bar

X

The Search bar allows the user to enter keywords related to the desired documents. The user enters one or more keywords and clicks the Search button or presses the "Enter"

key on the keyboard to perform the search. Results of the search are displayed in the Search Results list.

3

## Search Results List

Results:

---

### [Contingency Plan Template - NIST](#)

Contingency Plan Template - NIST

This document provides a NIST template for preparing a contingency plan. Downloaded from: <http://csrc.nist.gov/groups/SMA/fasp/documents/documtemplate.doc>.

ContingencyPlan\_template\_NIST.pdf

---

### [Contingency Plan Template for Systems - HHS](#)

Contingency Plan System Template - HHS

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

ContingencyPlan-system\_template\_HHS.pdf

---

### [Information Technology \(IT\) Contingency Plan Template - HHS](#)

Contingency Plan IT Template - HHS

This document is a template for an information technology (IT) contingency plan. It was targeted to the Dept. of Health and Human Service. Downloaded from: [http://www.hhs.gov/ocio/epic/Enterprise%20Performance%20Lifecycle%20Artifacts/epic\\_artifacts.html](http://www.hhs.gov/ocio/epic/Enterprise%20Performance%20Lifecycle%20Artifacts/epic_artifacts.html).

ContingencyPlan-IT\_template\_HHS.pdf

---

### [Contingency Planning Guide for Information Technology Systems \(Rev. 1\)](#)

NIST SP800-34 Contingency Planning

The Search Results list displays the documents found by the Search. Once there are documents displayed, the user can click a document to see the contents in a new tab.

## Wildcards

There are two different types of wildcard characters that can be used in the search. The first is the asterisk character that can be used to substitute for one or more characters. For example, if entering the text "fire\*", the search would look for anything starting with those characters and the user would see a prioritized list starting with topics related to firewalls. Without the asterisk the search would look for "fire" and the first entry would be Fire Protection.

Exact characters could also be substituted with question marks. For example, entering the text "NIST SP800-???" will return the NIST Special Publication 800 series documents where the last two characters are substituted by the wildcard character.

**When CSET is searching for the text string, it is evaluating both the title and the content of the document. While the search will evaluate any character string, it is recommended that the entry be as specific as possible to limit and refine the list. The search is not sophisticated enough to find similar or close spellings. A misspelled word like "Ciber-Security" will return no results.**

## Topic Searches

In most cases, the user will be searching for a specific subject; however, the search capability can also be used to search for types of documents. In the example above, the returned document is a DHS recommended practice. By entering "recommended practice" in the search text box, the user can create a list of all the recommended practices developed by DHS as well as other documents that may use that phrase.

## Browse Screen

Two ways are available to find documents within the Resource Library. The first is by using the document tree structure shown in the Figure below. The second is by using the Search screen discussed in the help section titled [Search Screen](#).

In the document tree structure, all the topics in the library are organized in a hierarchical format and displayed as leaf nodes on one or more branches, with a branch representing a topic. Each main topic can be expanded to more detailed subtopics until only the list of documents remains. The branches may be one or several levels deep.

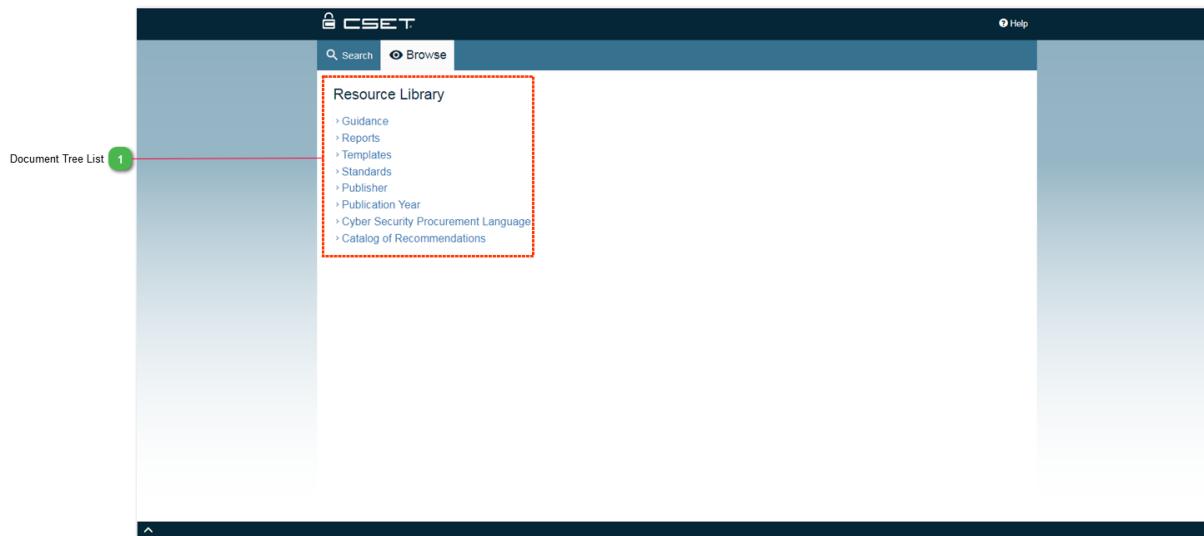


Figure: Resource Library Document Tree

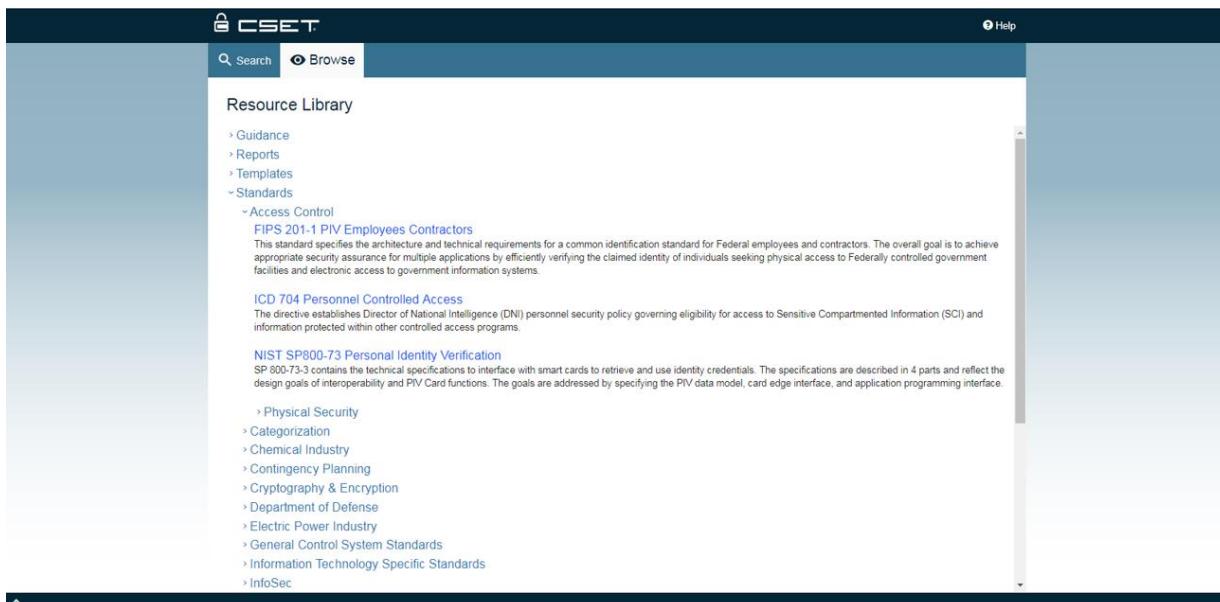
### 1 Document Tree List

#### Resource Library

- > Guidance
- > Reports
- > Templates
- > Standards
- > Publisher
- > Publication Year
- > Cyber Security Procurement Language
- > Catalog of Recommendations

The Document Tree list displays the documents in the Resource Library organized by category in an expandable tree structure. The tree structure contains branches (Categories) and Leaves (Documents). Branches can be clicked to show more branches

or leaves. Leaves can be clicked to display selected documents in a new tab.



**Figure: Expanded Document Tree**

In the example shown in the Figure above, the Access Control branch under Standards was clicked to open and expose the documents that are found under it. Any document selected will open in a new tab for the user to read.

The options to browse by publisher and publication year are also available. They were added for those users looking for specific versions of documents or documents from a specific source. The documents listed under these headings are the same as in the rest of the tree but listed in a differing order.

The final two subjects in the tree labeled Cyber Security Procurement Language and Catalog of Recommendations are unique and will open special access to the content rather than the files themselves.

### **Cyber Security Procurement Language:**

By clicking the branch labeled Cyber Security Procurement Language, the screen expands the tree to show the topics in the Procurement Language document. (The full document can be found using the Search or Document Tree methods.) The Figure below shows the branch open with the topic Removal of Unnecessary Services and Programs displayed (found under the System Hardening category).

The screenshot shows a section titled "Removal of Unnecessary Services and Programs". It includes several subsections: "Basis", "Language Guidance", and "Procurement Language". Each subsection contains detailed text and requirements. A small "OK" button is visible at the bottom left.

**Removal of Unnecessary Services and Programs**

System hardening is a security principle that should be considered when designing and procuring control systems products. It refers to making changes to the default configuration of a Network Device and its operating system (OS), software applications, and required third-party software to limit security vulnerabilities. Removal of unnecessary services and programs is an aspect of system hardening that refers to removal of unnecessary services and programs commonly installed on network devices.

**Basis**

Unused services in a host operating system that are left enabled are possible entry points for exploits on the network and are generally not monitored because these services are not used. Only the services used for control systems operation and maintenance shall be enabled to limit possible entry points.

**Language Guidance**

Often, networked devices ship with a variety of services enabled and default operating system programs/utilities pre-installed. These range from system diagnostics to chat programs, several of which have well-known vulnerabilities. Various attacks have been crafted to exploit these services to obtain information leading to compromise the system.

Any program that offers a network service that "listens" on specific addresses for connection requests. On a Transmission Control Protocol (TCP)/Internet Protocol (IP) network, these addresses are a combination of IP address and TCP or User Datagram Protocol (UDP) ports. A recommended hardening activity is simply disabling or removing any services or programs, which are not required for normal system operation, thus removing potential vulnerabilities.

Port scans are the normal method of ensuring existence of required services and absence of unneeded services. A port scan shall be run before the FAT with a representative, fully functional system configuration. All input/output (I/O) ports need to be scanned for UDP and TCP. The scan needs to be run before the FAT and again prior to the SAT. Port scans can rarely be used on production systems. In most cases, scanners will disrupt operations.

**Procurement Language**

*Postcontract award, the Vendor shall provide documentation detailing all applications, utilities, system services, scripts, configuration files, databases, and all other software required and the appropriate configurations, including revisions and/or patch levels for each of the computer systems associated with the control system.*

*The Vendor shall provide a listing of services required for any computer system running control system applications or required to interface the control system applications. The listing shall include all ports and services required for normal operation as well as any other ports and services required for emergency operation. The listing shall also include an explanation or cross reference to justify why each service is necessary for operation.*

**OK**

### Figure: Cyber Security Procurement Language

In this case, instead of a document being opened, CSET displays formatted text taken directly from the Cyber Security Procurement Language document.

Each topic includes some or all the following sections:

- Brief Overview of the Topic,
- Basis,
- Language Guidance,
- Procurement Language,
- Factory Acceptance Test (FAT) Measures,
- Site Acceptance Test (SAT) Measures,
- Maintenance Guidance,
- Dependencies, and
- References.

To fully understand how the procurement language was developed, how it is to be used, any limitations and constraints, and general information about the document, open the document and read the front pages. To access it, click on Search and then type in procurement language.

### Catalog of Recommendations:

This first level branch will open the list of topics that are associated with the Catalog of Control Systems Security: Recommendations for Standards Developers. The Figure below shows an example.

**Security Policy and Procedures**

Security policies are an extension of higher-level organizational policies with consideration for identified risks. Procedures implement the policies and allow the organization to communicate to employees, third party contractors, and vendors how the security program will be managed.

**Requirement**

The organization develops, implements, and periodically reviews and updates:

1. A formal, documented, control system security policy that addresses:
  1. The purpose of the security program as it relates to protecting the organization's personnel and assets
  2. The scope of the security program as it applies to all organizational staff and third-party contractors
  3. The roles, responsibilities, management commitment, and coordination among organizational entities of the security program to ensure compliance with the organization's security policy and other regulatory commitments.
2. Formal, documented procedures to implement the security policy and associated requirements. A control system security policy considers controls from each family contained in this document.

**Supplemental Guidance**

The security policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The control system security policy can be included as part of the general security policy for the organization. Procedures can be developed for the security program in general and for the control system in particular, when required.

**Requirement Enhancements**

None

**References**

NIST Special Publication 800-53 Revision 3 AC-1, SC-14, PM-1  
20 Critical Security Controls Twenty Critical Controls for Effective Cyber Defense: Consensus Audit CC-9

**OK**

**Figure: Catalog of Recommendations**

Development of the Catalog was originally sponsored by DHS with input from NIST and five national laboratories. It consolidated the requirements from 15 control system and information technology Standards and was intended to serve as a source of requirements and controls for the developers of ICS Standards. Because of its popularity and comprehensive ICS requirements, it has become a principal Standard in all versions of CSET and in the ICS community at large in addition to Standards developers.

To access a topic, simply click on the branch title in the tree. In the example above, Security Policy was selected and the topic Security Policy and Procedures was chosen.

On the right-hand side of the screen, CSET displays the content from the Catalog.

Each topic includes some or all the following sections:

- Brief Overview of the Topic,
- Requirement Text,
- Supplemental Guidance,
- Requirement Enhancements, and
- References.

Like the procurement language document, to fully understand the background and intent of the Catalog, open and read the front pages.

# User Profile

The User Profile menu allows the user to view their User Profile Information and their assessments, Change Password, and Logout of CSET.

The "My Assessments" link will navigate the user to their landing page. To learn more about the landing page, see Start Assessment Preparation.

The "Logout" link will log the user out and return them to the CSET home page.

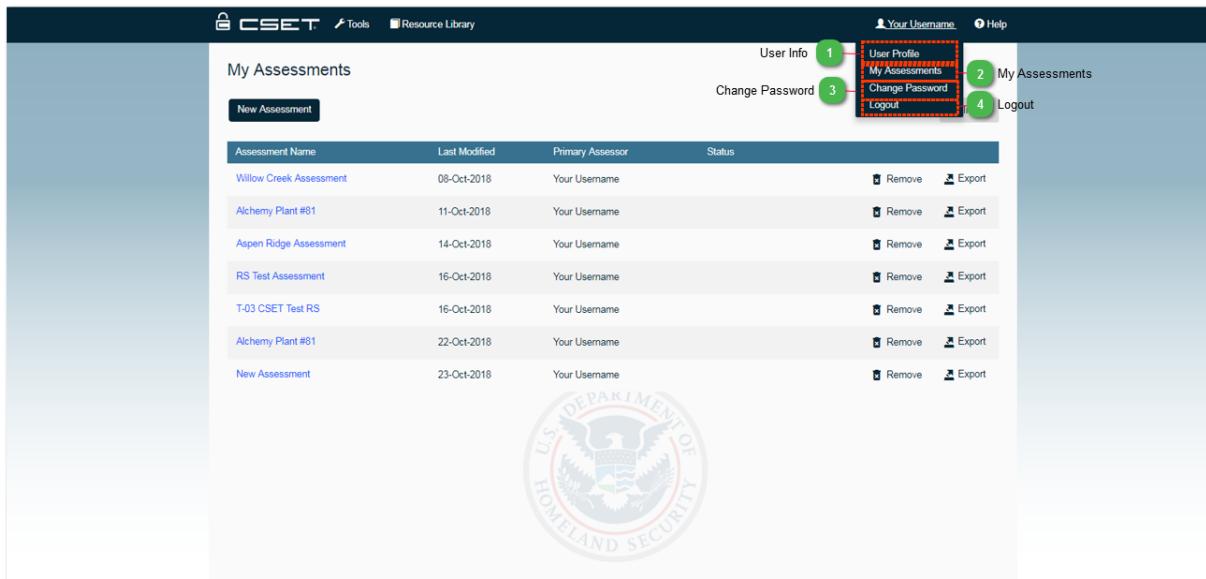


Figure: User Profile menu

1

## User Info

User Profile

Click User Profile to view and edit User Profile Information.

See [User Profile Information](#) for more information.

2

## My Assessments

My Assessments

Click My Assessments to be directed to the user's Landing Page.

See [CSET Landing Page](#) for more information.

3

## Change Password

Change Password

Click Change Password to change the user's password.

See [Change Password](#) for more information.

4

## Logout

[Logout](#)

Click Logout to be logged out of CSET and returned to the Home Page.

## User Profile

The User Profile menu allows the user to change their First Name, Last Name, and/or Email.

### Edit User Profile

First Name \*

Last Name \*

Email \*

Confirm Email \*

Providing security questions is optional but will allow you to recover your password should you forget it.

Security Question	Security Answer
What was the house number and street name you lived in as a child? ▾	160 childs ave
What is your first pet's name?	Spike

**Save** **Cancel**

**Figure: Edit User Profile dialogue**

The User Profile dialogue will show your profile information. Use this dialogue to change first and last name or email. Select the "Save" button to keep changes or "Cancel" to exit the dialogue.

## Change Password

Users can select the "Change Password" link to change their password.

Enter the Current Password, and New Password twice to change passwords.

The screenshot shows a modal dialog titled "Change Password". It contains three input fields: "Current Password \*", "New Password \*", and "New Confirm Password \*". Below the fields are two buttons: "Change Password" (in a dark blue box) and "Cancel".

Change Password	
Current Password *	<input type="text"/>
New Password *	<input type="text"/>
New Confirm Password *	<input type="text"/>
<input type="button" value="Change Password"/>	<input type="button" value="Cancel"/>

Figure: Change Password dialogue

## Help Menu

The Help Menu shown in the Figure below allows the user to access help documentation for the CSET tool.

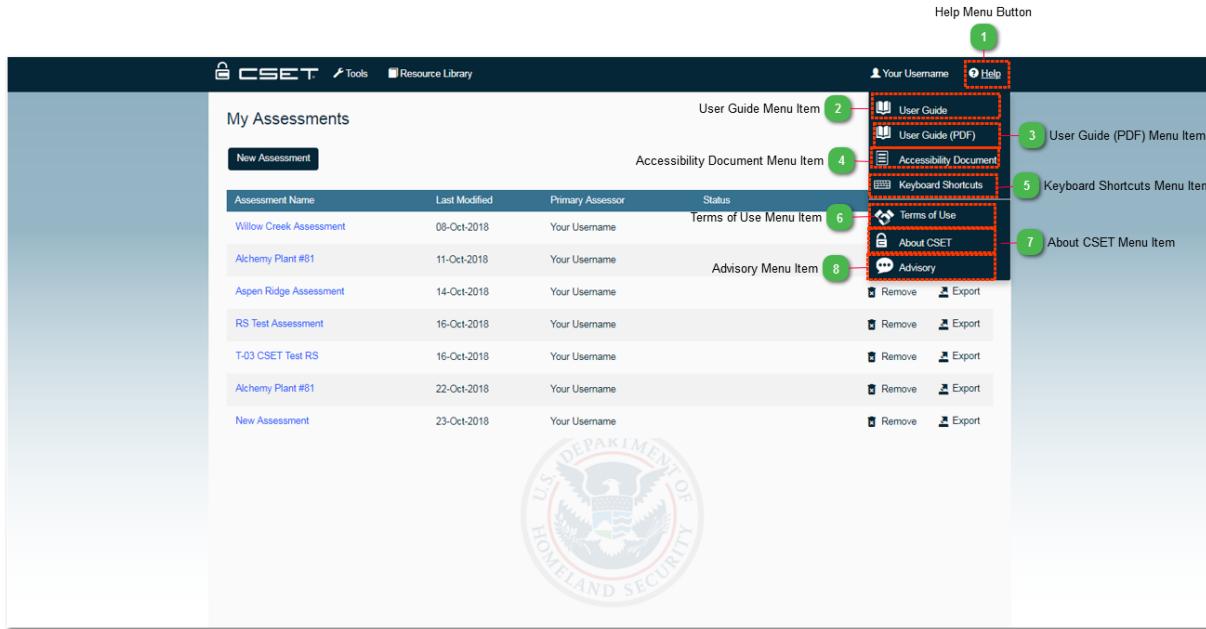


Figure: Help Menu

1

### Help Menu Button



Clicking the Help menu button opens the Help menu.

2

### User Guide Menu Item



Clicking the User Guide menu item will open this user guide as a CHM file containing screen shots and instructional information for using the CSET tool.

3

### User Guide (PDF) Menu Item



Clicking the User Guide (PDF) menu item will open this user guide as a PDF file containing screen shots and instructional information for using the CSET tool.

4

## Accessibility Document Menu Item

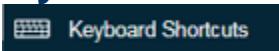


Clicking the Accessibility Document menu item will open the CSET Accessibility Features Document, which describes how CSET addresses accessibility issues including the use of screen readers, high contrast mode, and keyboard access.

See [Accessibility Document](#) for more information.

5

## Keyboard Shortcuts Menu Item

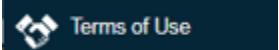


Clicking the Keyboard Shortcuts menu item will open the CSET Keyboard Shortcuts document, which contains a list of all keyboard shortcuts available to users of the CSET tool.

See [Keyboard Shortcuts](#) for more information.

6

## Terms of Use Menu Item



Clicking the Terms of Use menu item will open the CSET Terms of Use that describes the terms that user's agree to when using CSET.

See [Terms of Use](#) for more information.

7

## About CSET Menu Item



Clicking the About CSET menu item will open the About CSET window containing version information, web site links to videos, training and contact information for the CSET team.

See [About CSET](#) for more information.

8

## Advisory Menu Item



Clicking the Advisory menu item will open the Advisory window that contains disclaimer information.

See [Advisory](#) for more information.

## CSET ACCESSIBILITY FEATURES

The Figure below shows the CSET Accessibility Features document that can be accessed from the Help menu of the CSET tool.

**CSET Accessibility Features**

The features and functions within CSET have been developed to support application users with accessibility requirements. Industry standards have been followed to take advantage of accessibility features built into the Windows 7 operating system and the .NET architecture. These combined capabilities support compliance with Section 508 of the U.S. Rehabilitation Act.

**Analysis:** Accessibility for the analysis functionality can be accomplished by printing the reports or producing an on-screen version of the reports. Reports are generated in .HTML format.

**High Contrast Functionality**

All text areas on CSET other than the Diagram and Analysis pages support switching to High Contrast mode within the Windows operating system.

**Keyboard Access**

CSET is accessible from the keyboard. All areas of the application other than the Analysis page can be accessed from the keyboard. Most keyboard access is implemented by using the TAB and ARROW keys for navigation, the SPACE and ENTER keys for selection. Additional shortcut or hot keys may be found in the Keyboard Shortcuts dialog.

**Figure: CSET Accessibility Features Document**

## Keyboard Shortcuts

The Figure below shows the CSET Keyboard Shortcuts document that can be accessed from the Help menu of the CSET tool.

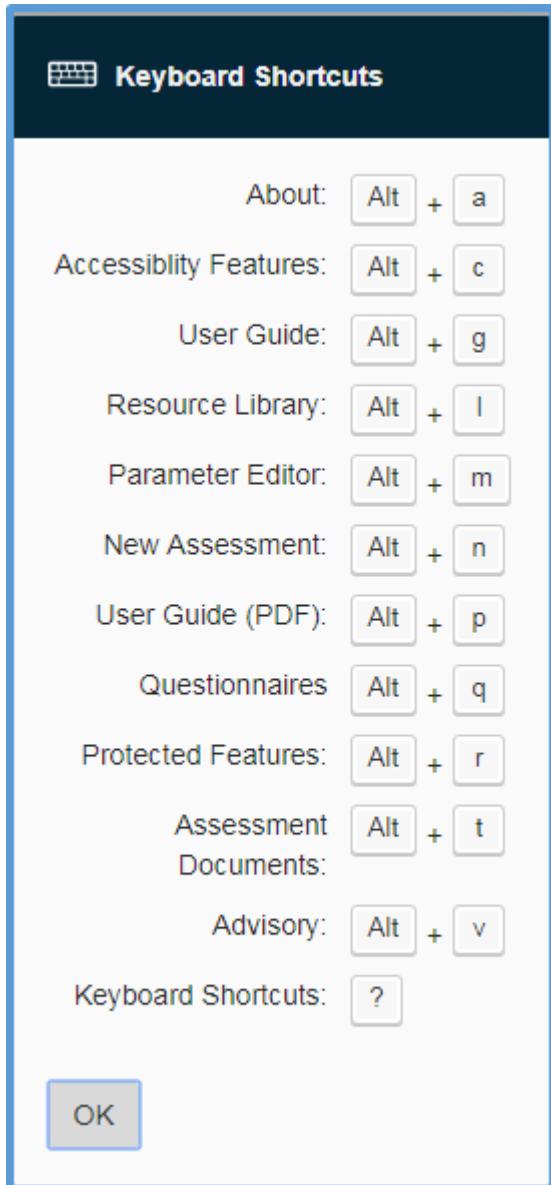


Figure: CSET Keyboard Shortcuts Document

## Terms of Use

The Figure below shows the Terms of Use that can be accessed from the Help Menu.



**Figure: Terms of Use**

## About CSET

The About CSET window provides the user with more information about the CSET team. The Figure below points out a few important details on the About CSET window.

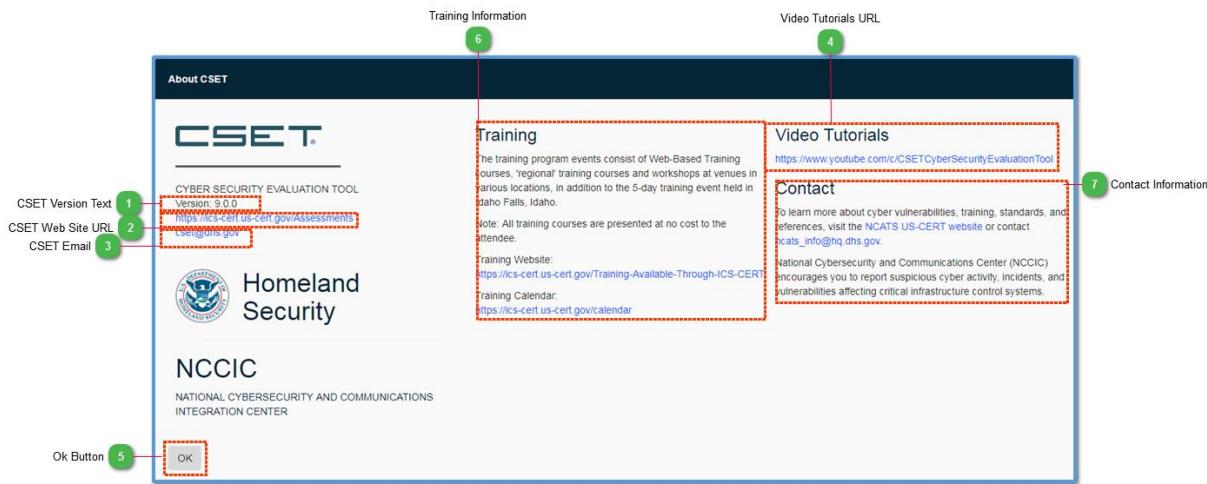


Figure: About CSET Window

**1**

### CSET Version Text

**Version: 9.0.0**

The CSET Version text indicates the current installed version of CSET. The last 4 digits indicate the build number that may be useful when communicating problems with the CSET support team.

**2**

### CSET Web Site URL

<https://ics-cert.us-cert.gov/Assessments>

The CSET Web Site URL is the CSET tool's web site URL where the user can learn more about the CSET tool, request features, and report defects or problems.

**3**

### CSET Email

[cset@dhs.gov](mailto:cset@dhs.gov)

The CSET email address allows the user to contact the CSET team with questions or concerns regarding the CSET tool.

**4**

### Video Tutorials URL

#### Video Tutorials

<https://www.youtube.com/c/CSETCyberSecurityEvaluationTool>

The Video Tutorials URL is a URL to current CSET training videos located on YouTube.

5

## Ok Button

 OK

Clicking the Close button will close the About CSET window

6

## Training Information

### Training

The training program events consist of Web-Based Training courses, 'regional' training courses and workshops at venues in various locations, in addition to the 5-day training event held in Idaho Falls, Idaho.

Note: All training courses are presented at no cost to the attendee.

Training Website:

<https://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT>

Training Calendar:

<https://ics-cert.us-cert.gov/calendar>

Use the links in Training Information to find training opportunities.

7

## Contact Information

### Contact

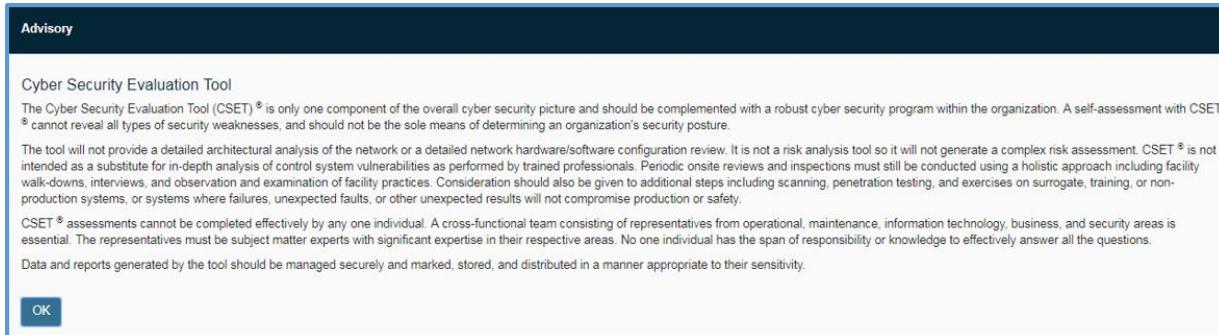
To learn more about cyber vulnerabilities, training, standards, and references, visit the [NCATS US-CERT website](#) or contact [ncats\\_info@hq.dhs.gov](mailto:ncats_info@hq.dhs.gov).

National Cybersecurity and Communications Center (NCCIC) encourages you to report suspicious cyber activity, incidents, and vulnerabilities affecting critical infrastructure control systems.

Use the links to contact a \_\_\_ representative for questions about....

## Advisory

The Figure below shows the Advisory window that can be accessed from the Help menu of the CSET tool.



**Figure: Advisory Screen**

## Operation Menus

This section addresses the main operation menus of the CSET assessment tool. They include the Preparation menu, the Assessment menu, and the Results menu.

## Preparation Menu

The Preparation menu allows quick access to the assessment preparation screens. The Figure below describes the buttons and menu.

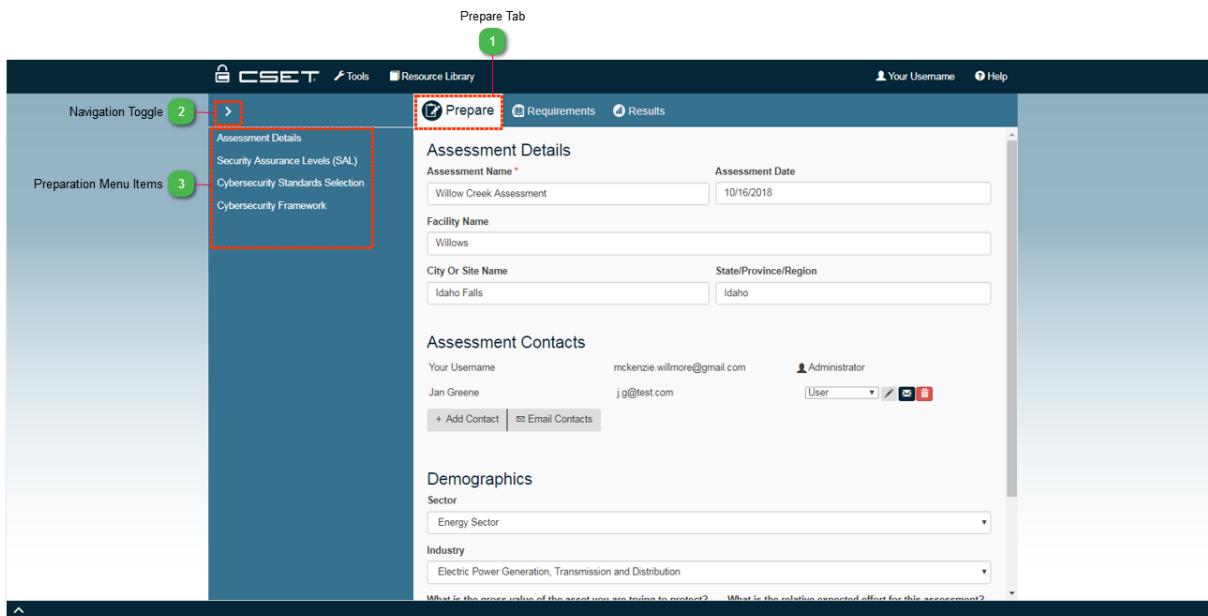


Figure: Preparation Button/Menu



Clicking the Preparation button will display the Assessment Details screen.

See [Assessment Details](#) for more information.



Use the Navigation Toggle to open and close the Navigation Menu.

3

## Preparation Menu Items

- Assessment Details
- Security Assurance Levels (SAL)
- Cybersecurity Standards Selection
- Cybersecurity Framework

The Preparation menu items indicate the screens encountered by the user during the preparation process.

See [Assessment Details](#), [Security Assurance Levels \(SAL\)](#), [Cybersecurity Standards Selection](#), and [Cybersecurity Framework](#) for more information.

## Questions Menu

The Questions menu allows quick access to the assessment questions and categories. The Figure below shows the Questions menu navigation.

NOTE: Requirements mode navigation will differ in that it shows standards at the top level and then categories nested underneath them.

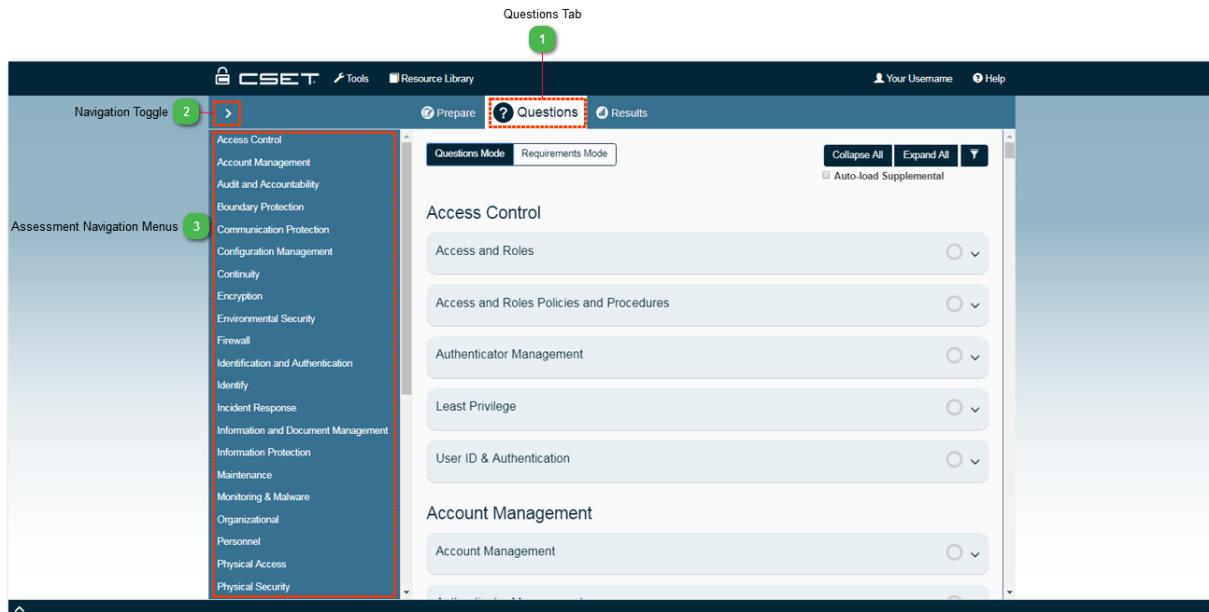


Figure: Assessment Button/Menu

1

### Questions Tab



Clicking the Questions Tab will display the Questions screen displayed after the Preparation process.

See the [Assessment Section](#) for more information about the Questions screen.

2

### Navigation Toggle



Use the Navigation Toggle to open and close the Navigation Menu.

3

### Assessment Navigation Menus



The Assessment Navigation menu shows a list of all question categories awaiting completion for the assessment. The user can quickly navigate to a specific category by clicking the desired menu item.

## Results Menu

The Results menu allows quick access to the assessment results and reports screens. The Figure below shows the Results menu.

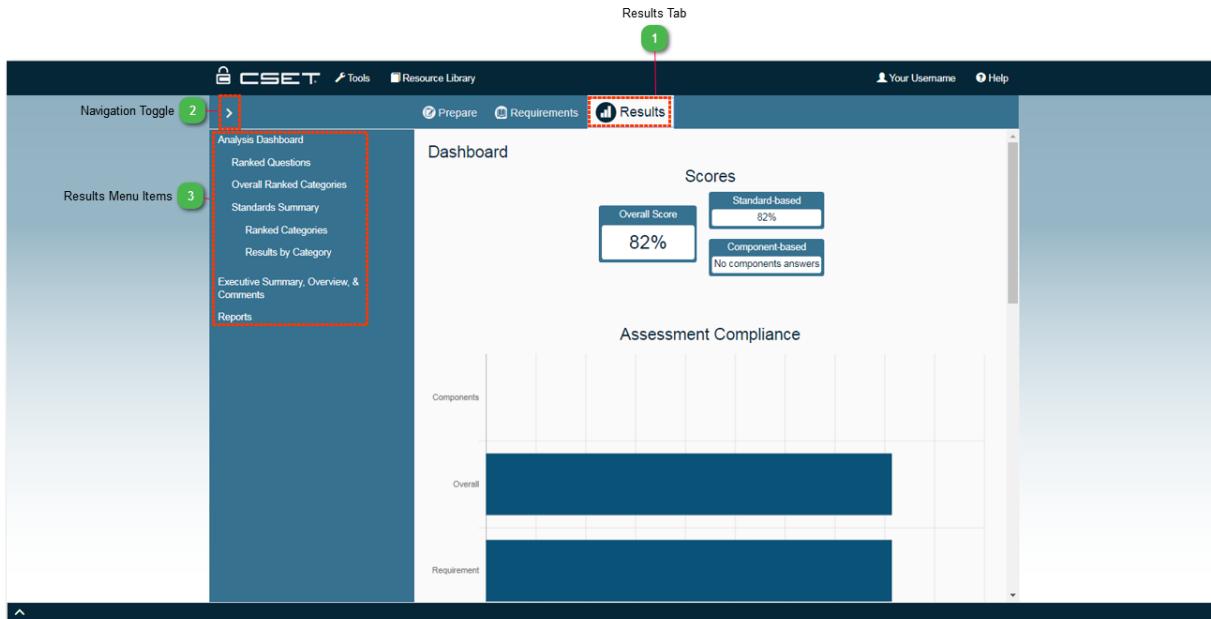


Figure: Results Button/Menu

1

### Results Tab



Clicking the Results button will display the Results Overview screen.

See the [Results Menu](#) for more information.

2

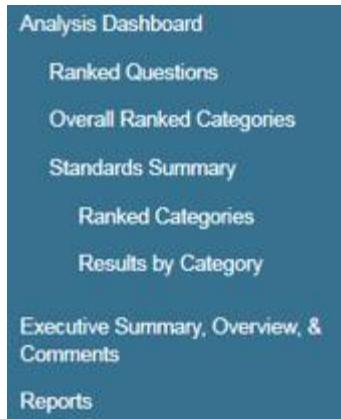
### Navigation Toggle



Use the Navigation Toggle to open and close the Navigation Menu.

3

### Results Menu Items



The Results menu items indicate the screens available to the user in the main Results Section.

## Main CSET Window Sections

This part of the user manual contains information about the different sections of the main CSET window including the Preparation, Assessment, and Results sections.

### Prepare Section

The Prepare section is where the assessment process begins. The preparation screens help the user to quickly get ready to answer the appropriate questions for their facility by defining the questions that will be answered during the assessment. The following pages will describe the preparation screens in more detail.

### CSET Landing Page

The CSET Landing page is the first screen seen after logging in. The Figure below shows the CSET Landing Page.

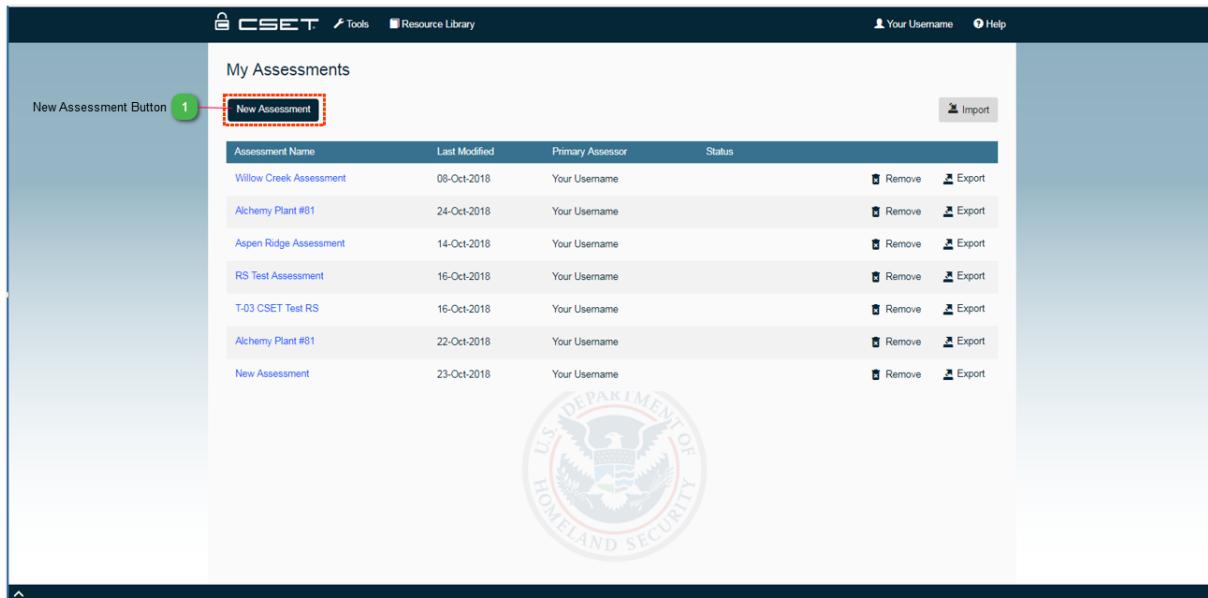


Figure: CSET Landing Page

1

#### New Assessment Button

[New Assessment](#)

Clicking the New Assessment button will start the assessment preparation process that will allow the user to address important areas before they can begin answering questions.

The first screen of the assessment preparation process is the [Assessment Details screen](#).

Tip: All the Landing page columns can be sorted by clicking the arrow next to the column name.

## Site Information Screen

Clicking the Assessment Details menu item in the Preparation Menu opens the Assessment Details screen. This screen allows for collecting specific information about the assessment including who was responsible, when it occurred, what sites or facilities were involved, and both descriptive and summary information. To use the Assessment Details screen, simply enter textual data into the fields provided. The Figure below addresses the different parts of the Assessment Details screen.

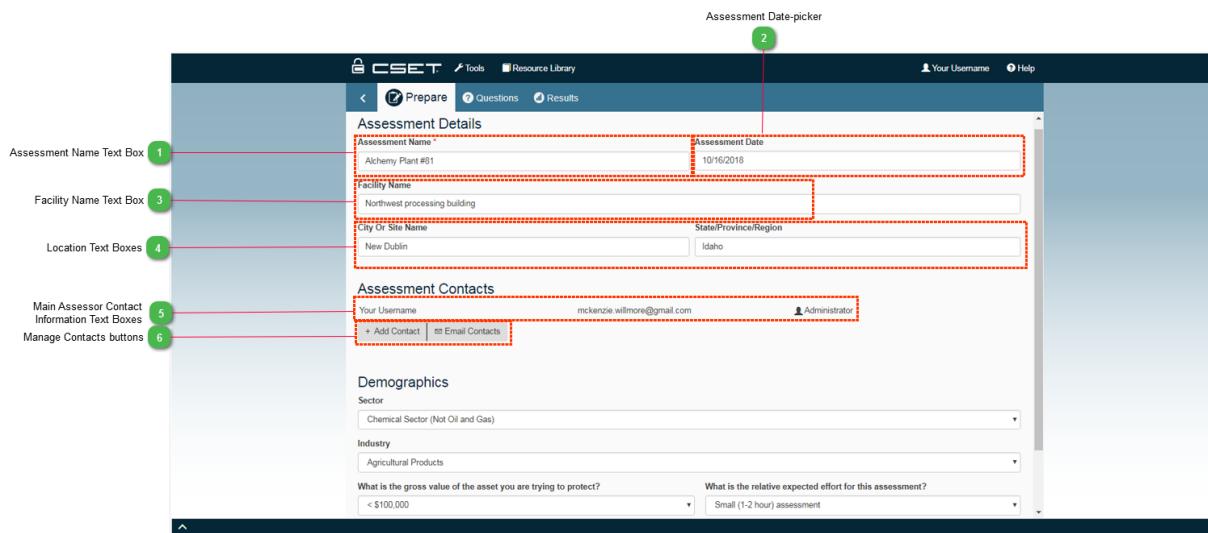


Figure: Assessment Details Screen

1

### Assessment Name Text Box

Assessment Name \*

Alchemy Plant #81

The Assessment Name text box is where the user enters the name of the assessment. The assessment name will also be displayed in the title area of the main CSET window and on the reports and will be used as the assessment file name if it isn't specifically changed by the user.

NOTE: An Assessment Name is required for CSET assessments. If the user hasn't provided one, CSET will name it "New Assessment".

2

### Assessment Date-picker

Assessment Date

10/16/2018

The Assessment Date-picker enables a user to add an initial date for the assessment. It requires a valid date format. Clicking the calendar icon will allow the user to select a date from a calendar control rather than entering the date manually.

3

## Facility Name Text Box

A screenshot of a web form showing a single input field labeled "Facility Name". The input field contains the text "Northwest processing building".

The Facility Name text box provides text input for identifying the name of the facility or facilities for which the assessment is created.

4

## Location Text Boxes

A screenshot of a web form showing two input fields: "City Or Site Name" containing "New Dublin" and "State/Province/Region" containing "Idaho".

The Location text boxes provide text input for identifying the name of the City or Site for which the assessment is created as well as the State, Province, or Region for which the assessment is created.

5

## Main Assessor Contact Information Text Boxes

A screenshot of a web form showing three input fields: "Your Username" containing "mckenzie.willmore@gmail.com", "Email" containing "mckenzie.willmore@gmail.com", and "Role" containing "Administrator".

The Assessor Contact Information text boxes display the contact information for the user that owns the assessment.

6

## Manage Contacts buttons

A screenshot of a web interface showing two buttons: "+ Add Contact" and "Email Contacts".

Clicking the Manage Contacts buttons allow the user to add contacts or invite contacts by email to an assessment.

For more information about managing contacts, see the [Contact Management](#) help section.

# Contacts Management

Contacts Management is handled within the Assessment Details screen. Find the Assessment Contacts section underneath Assessment Name, Date, etc. to begin.

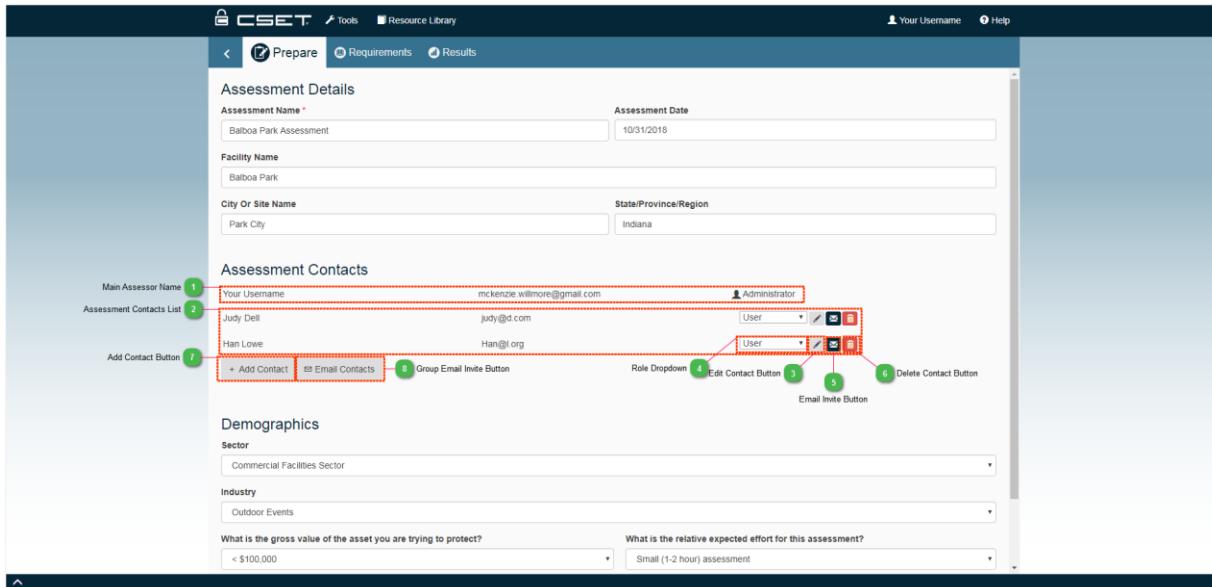


Figure: Contacts Management screen

1

## Main Assessor Name

Your Username

mckenzie.willmore@gmail.com

Administrator

The Main Assessor name field shows the user that created the assessment. They will always be listed at the top of the Contacts list.

2

## Assessment Contacts List

Judy Dell

judy@d.com

User   

Han Lowe

Han@l.org

User   

The Assessment Contacts list shows everyone that has been associated with the assessment.

3

## Edit Contact Button



Clicking the Edit Contact button makes the contact text field editable, so that changes can be made. Click the green arrow icon to commit changes.

Han

Lowe

Han@l.org

User



Figure. Contacts field in edit mode

4

## Role Dropdown



The Role dropdown allows the user to choose between "User" and "Administrator" rights for the contacts associated with their assessment.

Administrators can add and remove contacts to an assessment, and delete assessments. There must be an Administrator assigned to an assessment at all times.

5

## Email Invite Button



Clicking the Email Invite button will open up an email dialogue, so that users can customize their message.

A screenshot of a modal dialog titled "Invitation Email". The dialog contains fields for "From", "To", "Subject", and "Message", each with placeholder text. At the bottom are "Cancel" and "Send" buttons.

**From:** Your Username <mckenzie.willmore@gmail.com>

**To:**  
judy@d.com;  
Shows only those individuals that have not been sent an email

**Subject:**  
You have been invited to participate in a CSET assessment

**Message:**  
You have been invited to participate in a CSET assessment.  
Please log into your CSET account to participate. If you have not used CSET before, an account has been created for you, and a second email will be sent to this email address with instructions on logging in for the first time.

**Cancel** **Send**

Figure. Invitation Email dialogue

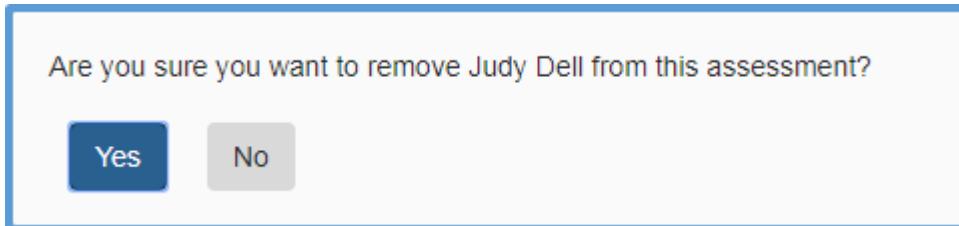
For the individual email invitation CSET will fill in the "To" field with the contact information with the user in the field next to the icon. The user can customize the email and hit "Send". After the email has sent the email icon changes to a .

6

## Delete Contact Button



Clicking the Delete Contact button brings up a confirmation dialogue.



**Figure. Contact Deletion dialogue**

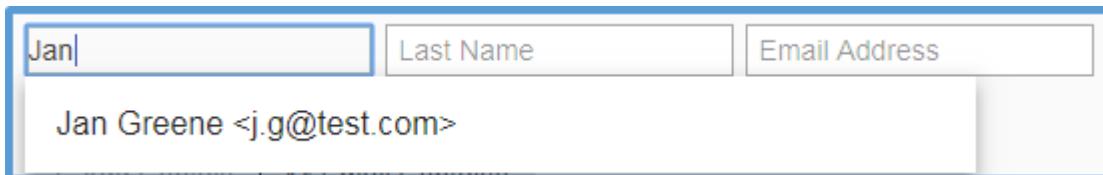
Selecting "Yes" will remove the contact from the assessment. Selecting "No" will keep the user associated with the assessment.

7

## Add Contact Button

+ Add Contact

Selecting the Add Contact button will open a text field to add the new contact's first, last name, and email, as well as, input their role. Select the  to commit the addition of the new contact. If the contact has previously been on an assessment with you before then the fields will auto-populate.



**Figure. Contact Auto-populate**

Click the user to complete the remaining fields.

When a user is added to an assessment they are sent an email inviting them to that CSET assessment. If they haven't yet registered for a CSET account they will be sent an additional email to walk them through the registration process.

8

## Group Email Invite Button

 Email Contacts

Clicking the Email Contacts button will open an email dialogue (the same as the individual email invitation). However, this email will include anyone in the contacts list that hasn't been sent an email yet. Customize the email (including the contacts receiving it) then click "Send".

All users that were sent the email will have a  next to their name.

## Sector and Demographic Information Screen

The Sector and Demographics Information screen collects sector and demographic information about the assessment. Completing these fields allows the CSET tool to help the user identify the appropriate Standards and questions that will be asked on the assessment. The Figure below describes the Sector and Demographic Information screen.

The screenshot shows the 'Sector and Demographic Information Screen' of the CSET tool. At the top, there are fields for Facility Name ('Willows'), City Or Site Name ('Idaho Falls'), and State/Province/Region ('Idaho'). Below these are sections for 'Assessment Contacts' and 'Demographics'. The 'Demographics' section is highlighted with a red dotted box and contains four dropdown lists: 'Sector' (with 'Energy Sector' selected), 'Industry' (with 'Electric Power Generation, Transmission and Distribution' selected), 'Asset Gross Value Drop Down List' (with '< \$100,000' selected), and 'Organization Size Drop Down List' (with 'Small (1-2 hour) assessment' selected). A 'Next' button is at the bottom right. Numbered circles (1 through 5) point to each of these four dropdown lists.

**Figure: Sector and Demographic Information Screen**

1

### Sector Drop Down List

The Sector drop down list contains a list of industry sectors. Users should select the sector most relevant to their industry.

2

### Industry Drop Down List

The Industry drop down list provides a list of industries relevant to the selected Sector. Once the user selects a Sector, the Industry drop down list will be populated with information relevant to the selected sector. Users should select the industry most relevant to their business.

3

### Asset Gross Value Drop Down List

What is the gross value of the asset you are trying to protect?

< \$100,000

The Asset Gross Value drop down allows the user to provide a rough dollar value estimate of the assets. CSET uses this information when determining the correct Standard to recommend to the user.

4

## Organization Size Drop Down List

What is the relative expected effort for this assessment?

Small (1-2 hour) assessment

The Organization Size drop down list allows the user to provide a rough estimate of the size of the organization. Available values are Small, Medium, and Large. CSET uses this information when determining the correct Standard to recommend to the user.

5

## Next Button

Next

Clicking the Continue button will navigate the user to the [Security Assurance Level \(SAL\) Selection](#) screen.

## Security Assurance Level (SAL) Selection

The Security Assurance Level or SAL is a measure that determines the level of rigor applied to the assessment and also determines the number of questions required for the assessment. This section provides information on the Security Assurance Level or SAL process, the different types of SALs available in CSET, and the options for selecting the correct SAL for the current assessment.

### Standard SAL Selection

The Standard SAL Selection window allows the user to quickly and easily select the Security Assurance Level for the assessment. This option is best for advanced users that know the appropriate SAL or CIA levels for their assessment and don't require assistance to determine the appropriate SAL. The Figure below shows the Standard SAL Selection screen.

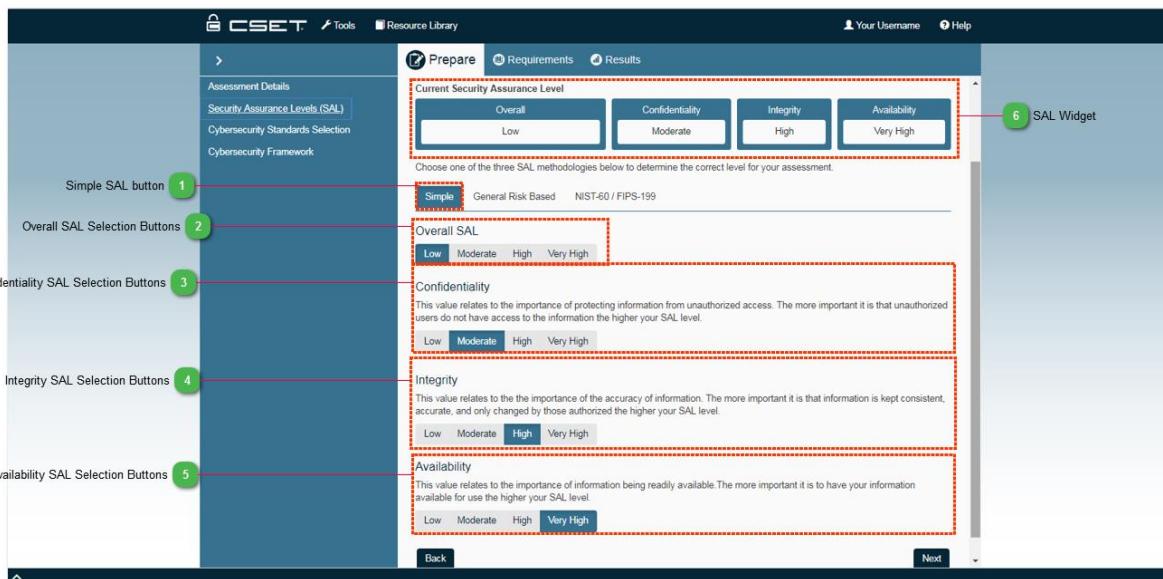


Figure: Standard SAL Selection Screen

1

#### Simple SAL button

The Simple SAL button is blue when selected. This indicates that the user is on the Simple SAL screen.

2

#### Overall SAL Selection Buttons

The Overall SAL Selection buttons allow the user to quickly and easily select the Overall SAL for the assessment. Simply select the appropriate level and then click the "Next" button to navigate to the next screen. The selected SAL will be saved and associated with the assessment.

The default SAL is Low. The available levels include:

- Low
- Moderate
- High
- Very High

Low, Moderate, and High correspond with the levels identified by NIST in the NIST SP800-53 Standards, the NIST SP800-60 Volumes 1 and 2 documents, and the Chemical Facility Anti-Terrorism Standards (CFATS) risk-based tiering structure. Very High is defined in CSET as comprising all controls including all optional enhancements. It is used to accommodate the multiple Standards available in CSET.

The levels of potential impact are defined as:

**Low:** The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

**Moderate:** The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

**High:** The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

**Very High:** A level of Very High is not defined in the NIST SP800-53 based Standards. It is included in CSET to accommodate the multiple Standards available in the tool and is defined as including all controls and all optional control enhancements.

3

## Confidentiality SAL Selection Buttons

### 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

The Confidentiality SAL Selection buttons allow the user to select the appropriate Confidentiality level if it is known. The overall SAL will be determined based on the highest level selected between the selected Confidentiality, Integrity, and Availability

levels.

4

## Integrity SAL Selection Buttons

### 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.

Low   Moderate   **High**   Very High

The Integrity SAL Selection buttons allow the user to select the appropriate Integrity level if it is known. The overall SAL will be determined based on the highest level selected between the selected Confidentiality, Integrity, and Availability levels.

5

## Availability SAL Selection Buttons

### Availability

This value relates to the importance of information being readily available. The more important it is to have your information available for use the higher your SAL level.

Low   Moderate   High   **Very High**

The Availability SAL Selection buttons allow the user to select the appropriate Availability level if it is known. The overall SAL will be determined based on the highest level selected between the selected Confidentiality, Integrity, and Availability levels.

6

## SAL Widget

### Current Security Assurance Level



The SAL Widget is a display only image that indicates to the user how their SAL selections are affecting the Overall SAL and CIA scores.

Tip: CSET only uses one of the SAL types. The highest SAL rating out of all of them is what the user's assessment will be based on.

## General SAL Selection

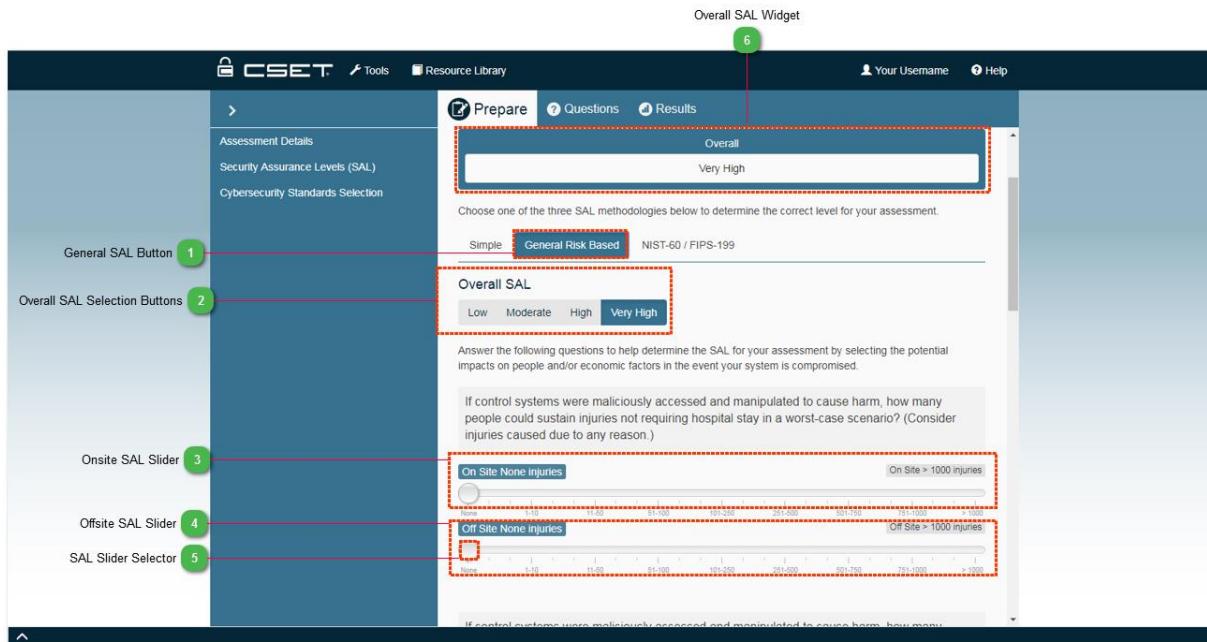
The General SAL Selection screen helps the user to determine the overall SAL for the assessment by selecting the potential impacts on people and economic factors in the event that systems are compromised. The General SAL Selection screen is described in the Figure below.

The General SAL approach is consequence based. To use the screen, simply move the sliders to align with the total number of people or total dollar amount impacted for each question and category. Answers should be provided for both onsite and offsite impact.

For example, to determine the numeric value for potential injury, estimate the number of people, (onsite at the facility or those affected offsite) who could be injured without the need for hospitalization, should the scenario occur.

Estimate a worst-case number by assuming a full work shift with the addition of any visitors, contractors, vendors, etc., who may also be onsite. For the offsite estimate, assume peak occupancy of affected areas. For example, if a business district will be impacted by an event, then plan the estimate during the primary business hours. Consider all aspects of the scenario such as chain reactions. An explosion could be followed by a fire that could then close roadways, or even release toxic materials.

When considering the money-based questions, consider all costs including legal fees, fines, penalties, replacement costs, compensation, etc.



**Figure: General SAL Screen**

1

### General SAL Button

**General Risk Based**

The General SAL button is blue when selected. This indicates that the user is on the General SAL screen.

2

## Overall SAL Selection Buttons

### Overall SAL

Low    Moderate    High    **Very High**

The Overall SAL Selection buttons allow the user to quickly and easily select the Overall SAL for the assessment. Simply select the appropriate level and then click the "Next" button to navigate to the next screen. The selected SAL will be saved and associated with the assessment.

The default SAL is Low. The available levels include:

- Low
- Moderate
- High
- Very High

Low, Moderate, and High correspond with the levels identified by NIST in the NIST SP800-53 Standards, the NIST SP800-60 Volumes 1 and 2 documents, and the Chemical Facility Anti-Terrorism Standards (CFATS) risk-based tiering structure. Very High is defined in CSET as comprising all controls including all optional enhancements. It is used to accommodate the multiple Standards available in CSET.

The levels of potential impact are defined as:

**Low:** The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

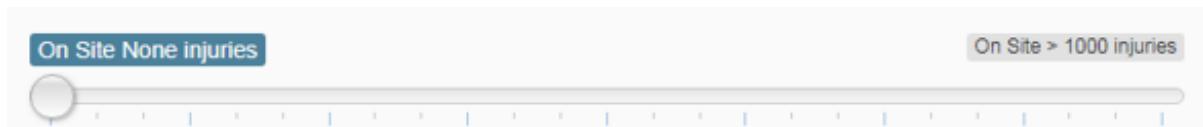
**Moderate:** The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

**High:** The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

**Very High:** A level of Very High is not defined in the NIST SP800-53 based Standards. It is included in CSET to accommodate the multiple Standards available in the tool and is defined as including all controls and all optional control enhancements.

3

## Onsite SAL Slider

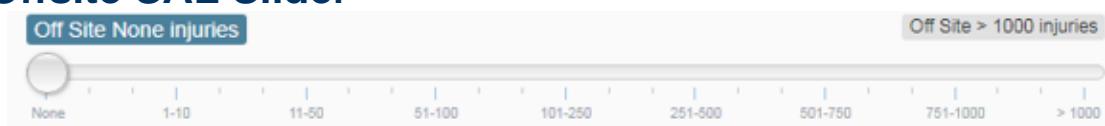


On-Site sliders indicate potential impacts to people or facilities that are on-site.

The user should estimate a worst-case number by assuming a full work shift with the addition of any visitors, contractors, vendors, etc., who may also be on site. All aspects of the scenario, such as chain reactions, should be considered. For example, an explosion could be followed by a fire that could then release toxic materials.

4

## Offsite SAL Slider



Off-Site sliders indicate potential impacts to people or facilities that are off site or in surrounding communities.

The user should estimate a worst-case number by assuming a maximum number of people present in the surrounding communities. All aspects of the scenario should be considered such as chain reactions. For example, an explosion could be followed by a fire which could then release toxic materials.

5

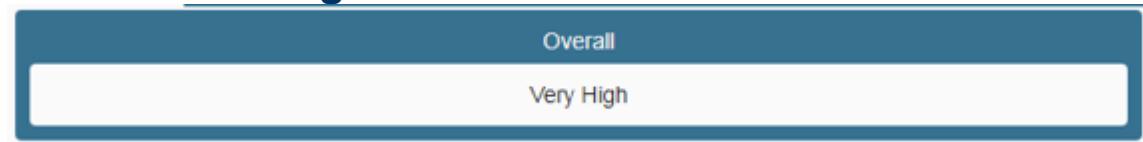
## SAL Slider Selector



The SAL slider selector is used to indicate the correct value assigned to the question. The overall SAL is determined based on the values of all SAL slider selectors on the screen.

6

## Overall SAL Widget



The SAL Widget is a display only image that indicates to the user how their SAL selections are affecting the Overall SAL.

Tip: CSET only uses one of the SAL types. The highest SAL rating out of all of them is what the user's assessment will be based on.

## General SAL – Injury

The slider bars provide a general range of values for both human and economic impact. The range of values is somewhat broad but allows for a uniform way of measuring the various categories. Review the question and move the slider to the best estimate of the answer.

### Onsite

Estimate the number of onsite people who could be injured (without the need for hospitalization) should the scenario occur.

Estimate a worst-case number by assuming a full work shift with the addition of any visitors, contractors, vendors, etc., who may also be on site. Consider all aspects of the scenario such as chain reactions. For example, an explosion could be followed by a fire, which could then release toxic materials.

### Offsite

Estimate the number of offsite people who could be injured (without the need for hospitalization) should the scenario occur.

Estimate a worst-case number by assuming a maximum number of people present in the surrounding communities. Consider all aspects of the scenario such as chain reactions. For example, an explosion could be followed by a fire, which could then release toxic materials.

## General SAL – Hospital

The slider bars provide a general range of values for both human and economic impact. The range of values is somewhat broad but allows for a uniform way of measuring the various categories. Review the question and move the slider to the best estimate of the answer.

### Onsite

Estimate the number of onsite people who could be injured and require hospitalization should the scenario occur.

Estimate a worst-case number by assuming a full work shift with the addition of any visitors, contractors, vendors, etc., who may also be on site. Consider all aspects of the scenario such as chain reactions. For example, an explosion could be followed by a fire, which could then release toxic materials.

### Offsite

Estimate the number of offsite people who could be injured and require hospitalization should the scenario occur.

Estimate a worst-case number by assuming a maximum number of people present in the surrounding communities. Consider all aspects of the scenario such as chain reactions. For example, an explosion could be followed by a fire, which could then release toxic materials.

## General SAL – Death

The slider bars provide a general range of values for both human and economic impact. The range of values is somewhat broad but allows for a uniform way of measuring the various categories. Review the question and move the slider to the best estimate of the answer.

### Onsite

Estimate the number of onsite people who could be killed should the scenario occur.

Estimate a worst-case number by assuming a full work shift with the addition of any visitors, contractors, vendors, etc., who may also be on site. Consider all aspects of the scenario such as chain reactions. For example, an explosion could be followed by a fire, which could then release toxic materials.

### Offsite

Estimate the number of offsite people who could be killed should the scenario occur.

Estimate a worst-case number by assuming a maximum number of people present in the surrounding communities. Consider all aspects of the scenario such as chain reactions. For example, an explosion could be followed by a fire, which could then release toxic materials.

## General SAL – Capital Assets

The slider bars provide a general range of values for both human and economic impact. The range of values is somewhat broad but allows for a uniform way of measuring the various categories. Review the question and move the slider to the best estimate of the answer.

### Onsite

Capital Assets are tangible property owned or used by the organization including buildings, structures, trailers, vehicles, machinery, utilities, office equipment, fixtures, furniture, and land.

Calculate the costs by multiplying the replacement cost of the asset by the estimated damage in percent.

### Offsite

Capital Assets are tangible property used by the surrounding communities such as buildings, structures, vehicles, transit systems, roads, bridges, machinery, utilities, livestock, agricultural products, home and business equipment, fixtures, furniture, and land.

Calculate the costs by multiplying the replacement cost of the property by the estimated damage in percent.

## General SAL – Economic Impact

The slider bars provide a general range of values for both human and economic impact. The range of values is somewhat broad but allows for a uniform way of measuring the various categories. Review the question and move the slider to the best estimate of the answer.

### Onsite

Economic impact includes costs because of loss of production, damage or loss of product or feed stock, damage or loss of control system logic (damage to the physical system components should be counted under capital assets), damage or loss of data, costs of lawsuits, etc.

To estimate the cost of production loss, divide the annual budget by 365 (to calculate the daily budget) then multiply by the estimated down time in days. Include an estimate of displacement costs. That is, the estimated cost of working from an alternate, temporary location such as using a rented trailer for administrative functions. The cost of lawsuits with the associated loss of reputation is difficult to estimate. Look to history for the occurrence of similar scenarios for an indication of economic impact.

### Offsite

Economic impact includes costs because of the communities' loss of supplies and services (food, power, water, medical services, etc.), loss of access to jobs, cost of emergency response actions, damage or destruction of agricultural land, etc.

Include an estimate of displacement costs for hospitals, schools, churches, and homes. The cost of lawsuits with the associated loss of reputation is difficult to estimate. Look to history for the occurrence of similar scenarios for an indication of economic impact.

## General SAL – Environmental Cleanup

The slider bars provide a general range of values for both human and economic impact. The range of values is somewhat broad but allows for a uniform way of measuring the various categories. Review the question and move the slider to the best estimate of the answer.

### Onsite

Estimate costs for direct and contract labor for cleanup and remediation, equipment, rentals, materials, waste disposal, permitting fees, investigation support, and fines.

Costs should be estimated for onsite impacts.

### Offsite

Estimate costs for direct and contract labor for cleanup and remediation of surrounding communities, equipment, rentals, materials, waste disposal, permitting fees, investigation support, and fines.

Costs should be estimated for the impacts to (offsite) communities.

## General SAL Considerations

The information here provides additional guidance for users in determining their General Security Assurance Level (SAL).

### Characterize Assets

This step identifies assets that, if compromised, have the potential to cause undesirable consequences. In addition, assets owned by the organization or in proximity of the compromised facility that could be open to danger should be identified.

The options and resources in the following list may be used, as appropriate, for determining assets:

- Assets identified in risk and vulnerability assessments;
- Capacity, operation, management, and maintenance manuals;
- Risk management program manual;
- Hazardous waste operations and emergency response Standards;
- Emergency operations plan, particularly event-escalation criteria;
- Y2K documentation, including asset inventory, criticality determination, contingency plans, etc.;
- Asset inventory and criticality rating in the Computerized Maintenance Management System (CMMS);
- Inventory list of process control/SCADA hardware, including interfaces;
- Safety incident reports indicating accidents or near misses;
- Area maps showing schools, businesses, residential areas, rivers, or other transport paths;
- Population distributions; and
- Wind and water flow maps.

### Define Worst-Case Scenarios

This step helps the assessment team acknowledge and consider the worst-case scenarios.

In defining worst-case scenarios, it is important to realize that many different ways are available to initiate a compromise of a control system. These include: (1) intentional, directed attacks with the intent of taking control of the system; (2) undirected attacks, such as viruses or worms, that can cause the system to malfunction; and (3) accidents that are caused by or result in inappropriate actions taken by an operator.

The worst-case scenarios should focus on the results, not the method, except as it relates to the compromise. In most cases, an undirected attack will cause problems, such as denial of service, which can shut down the control system and possibly prevent corrective action being taken. Directed attacks can result in an unauthorized person taking control of the system, and then opening or closing valves to create dangerous mixtures or release of materials to the environment.

The secondary consequences of a system compromise should also be considered in developing scenarios. For example, the loss of a power grid supplying power to a large population area

may cause a domino effect of further power loss to financial centers, businesses, transportation systems, and heating, cooling for homes, hospitals, schools, etc.

An example of a worst-case scenario might be the intentional and undetected opening of one or more valves causing the release of a toxic material to the atmosphere. The material could then be carried over to a nearby community resulting in injuries, fines, and environmental cleanup costs.

## **Estimate Consequences**

Ask these questions. If the identified scenarios were to occur, what would the consequences be to the organization including its customers and the surrounding community? How would the organization be impacted by the following?

- Personal health and safety (injury, loss of life);
- Loss of capital assets;
- Adverse environmental impacts; and
- Adverse economic impacts.

The guidelines in this section are provided to assist in estimating a value for the consequences of an undesired event. The guidelines are not prescriptive and do not replace current consequence estimating procedures that the organization may have in place. Each guideline presented in this section correlates to categories contained in questions to determine the SAL for both onsite and distributed assets.

Remember, for a worst-case scenario, select worst-case conditions.

## **Injury and Loss-of-Life Estimate**

Estimates for injury and loss of life can be challenging to determine. To estimate the number of people at risk for each scenario, consider the agents that would cause injury or death, their impact area, and the method of transport. Also, there may be several different agents for a single scenario, such as the force of an explosion, a subsequent fire, and the release of toxic materials.

The tool divides affected persons into two groups: personnel that are onsite and people that are outside the facility boundaries (i.e., people in the surrounding communities). Start by counting the number of people most likely to be onsite or in the area of the distributed asset, and then estimate the number of people outside the facility boundaries that could be affected. Different times of the day or different environmental conditions could exacerbate the situation.

The tool also breaks injuries into two categories: injuries that do not require hospital stay and injuries that do require hospital stay. For example, minor exposures to contaminants that can be treated with an eyewash or shower are not as serious as those requiring hospitalization because of a more serious exposure.

## **Capital Asset Loss Estimate**

Capital assets are tangible property used by the organization or community such as buildings, machinery, fixtures, furniture, and equipment.

To estimate the organizational capital asset loss, perform the following steps:

- Determine the total estimated value of each potentially impacted site or distributed asset for each example scenario. The following is a typical list of asset types to consider:
  - Buildings, including all structures that serve as buildings such as permanently established trailers.
  - Machinery and equipment, including all motor vehicles (licensed and nonlicensed), trailers, construction and maintenance equipment, fixtures, computers, and office furniture.
- Estimated structure losses (structure replacement value multiplied by the estimated damage in percent). For example, if a plant's structure replacement value equals \$100,000, and the expected damage is 40 percent of the structure, then the loss to this structure is \$40,000.
- Estimated content losses (content replacement value multiplied by the estimated damage in percent). For example, if the plant's content replacement value equals \$225,000, and the expected damage is 10 percent of the contents, then the losses to these contents are \$22,500.
- Structure and content loss are calculated as

*For each asset,*

$$\text{Structure loss (\$)} = (\text{structure replacement value}(\$)) \times (\% \text{ damage})$$

$$\text{Contents loss (\$)} = (\text{contents replacement value} (\$)) \times (\% \text{ damage})$$

To estimate the community capital asset loss,

- Estimate the value of capital assets that are within the impact area of the scenario and the estimated extent of damage to these capital assets. The same process described for determining organizational assets can be used for determining community assets.

## Environmental Impacts

Impacts to the environment can be wide ranging and have far-reaching consequences. These consequences may include cleanup, as a minimum, remediation, and investigations with fines from regulatory agencies. Calculate the environmental consequence by estimating costs for the following:

- Direct labor (for cleanup, remediation, etc.);
- Contractor (for cleanup, remediation, etc.);
- Equipment;
- Rented equipment;
- Materials;
- Fees for permits;
- Community mitigation efforts (e.g., portable toilets);
- Investigation support;
- Fines; and
- Material disposal.

## Economic Impact

The economic impact because of a worst-case scenario may include costs associated with loss of production, impact to reputation, damage or loss of finished product or feed stock, damage to or loss of the control system because of cyber damage requiring reprogramming of machines or rewriting of code, damage to the physical control hardware would be included under capital equipment, corrective action to prevent similar intrusions in the future, possible law suits, etc.

Losses associated with production are much easier to estimate than some other impacts. Production losses can be estimated using the following recommendations:

- Determine functional downtime or the time (in days) that the function would be disrupted because of the event.
- Estimate the average number of days various functions might be unavailable following a worst-case scenario occurrence.
- Estimate the daily cost of the functional downtime. Divide the average annual budget by 365 to determine the average daily operating budget or sales. Multiply the average daily operating budget by the functional downtime to determine the cost of the loss of function for the period that the service was unable to operate because of the event. For example, if a plant has an annual budget of \$6,000,000 and an average daily budget of \$16,438 (\$6,000,000/365), the losses could be estimated by using the annual budget as a proxy for the value of the service to the community. For example, if the plant were down for 7 days, then the cost for the loss of use for 7 days would be \$115,066 (\$16,438×7).
- Determine the displacement time, or the time in days, that a function may need to operate from a temporary location, if applicable. For example, if the administration building is inaccessible for 7 days (functional downtime) and operations are resumed from a trailer for the next 90 days, then the displacement time would be 90 days. Not all functions would require displacement before resuming operation.
- Multiply the displacement cost by the displacement time to determine the cost of the displacement from the regular place of business, as:

*For each asset, structure use and function loss =  
(average daily operating budget (\$)) × (functional downtime (# of days)) +  
(displacement cost per day (\$)) × (displacement time (# of days))*

Loss of finished product and feed stock can be estimated by using historical accounts of the amount of product kept onsite at any time. This may be either a maximum (worst case) or an average amount. The cost of the feed stock would be the replacement cost. If not having the feed stock on hand impacts the ability to restart the system, this would also affect loss of production. The loss of finished product would be the cost of producing the lost amount of the finished product. This could be determined by using production history as well.

The cost of cyber damage to the control system must be estimated based on what is most likely to be affected according to the scenario. The scenario may require the control system software to be rebuilt or the control code to be reworked, or it may require that an antivirus program be run on the system. The cost of this effort needs to be estimated. It may also require investigation of what caused the problem and the costs of reworking the system in order to implement a fix.

The economic impact because of loss of reputation or lawsuits is much harder to estimate.

History of similar incidents either within the organization or within similar organizations might provide an indication of the potential economic impact.

## **EVALUATE TOTAL IMPACT**

After evaluating each of the consequences and their costs, determine if areas are either counted twice or might mitigate or enhance the impact of the individual consequences. These may need to be adjusted. With these final figures, answer the questions for determining the SAL.

## FIPS 199 SAL Selection

After clicking the FIPS 199 SAL Determination link on the top pill navigation of the SAL screen, the display will change to that shown in the Figure below. This Instructions page provides links to a guide and the source documents.

The process is based on the Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems* and the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*. These Standards apply to information within the US federal government and federal information systems.

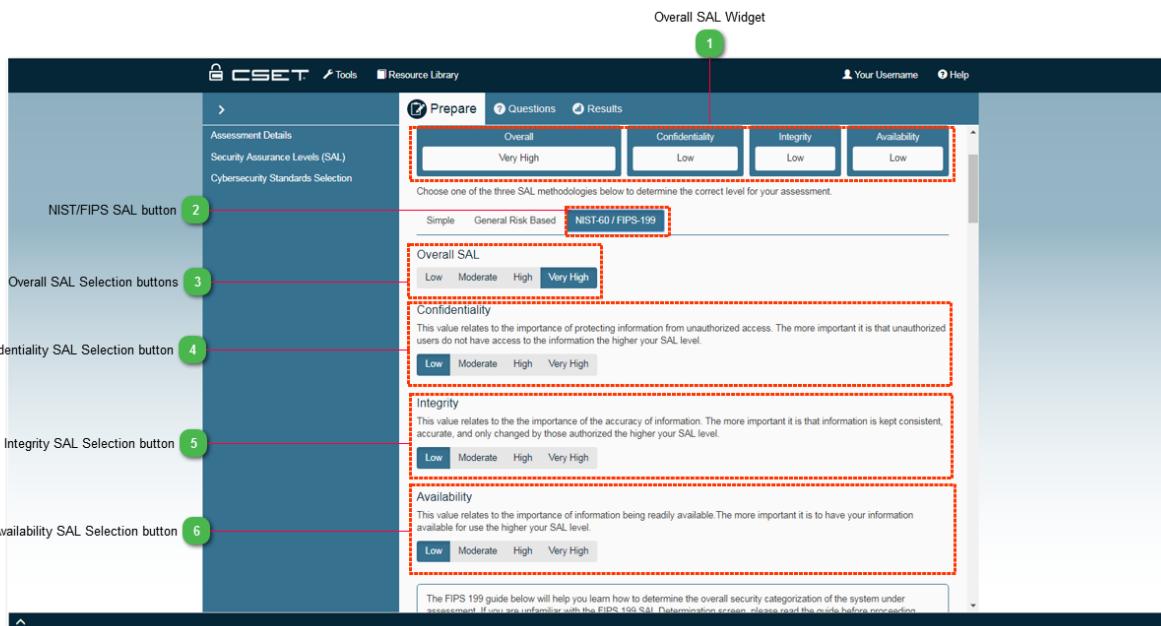


Figure: FIPS 199 SAL Screen

**Select Information Types:** After selecting your SAL levels, the next step is to check all applicable information types.

CIA Values Based on Selected Information Types			
Check applicable information types.			
Type	C	I	A
<input type="checkbox"/> Air Transportation : D.11.3	LOW	LOW	LOW
<input type="checkbox"/> Asset and Liability Management : C.3.2.1	LOW	LOW	LOW
<input type="checkbox"/> Budget Execution : C.2.3.5	LOW	LOW	LOW
<input type="checkbox"/> Budget Formulation : C.2.3.1	LOW	LOW	LOW
<input type="checkbox"/> Budgeting & Performance Integration : C.2.3.8	LOW	LOW	LOW
<input type="checkbox"/> Capital Planning : C.2.3.2	LOW	LOW	LOW
<input type="checkbox"/> Collections & Receivables : C.3.2.6	LOW	MOD	LOW
<input type="checkbox"/> Contingency Planning : C.2.4.1	MOD	MOD	MOD

**Figure: Selected Information Types Tab**

When an information type is selected in the list on the left of the screen, CSET displays that type with the values in the block on the right and at the same time dynamically updates the combined values in the block on the top, including the overall SAL.

No specific definition is given for each information type in CSET. To understand how the types are broken out the guidance documents discussed above must be opened.

**Answer Questions:** The next step in determining the SAL using the FIPS 199 method is to answer a short set of questions that may adjust the level in one or more of the categories. Figure # shows the screen when the Answer Questions tab has been clicked.

Answer Questions	
Does aggregation of information on this system reveal sensitive patterns and plans, or facilitate access to sensitive or critical systems?	<input type="button" value="Yes"/> <input checked="" type="button" value="No"/>
Does/could access to this system result in some form of access to other more sensitive or critical systems (e.g., over a network)?	<input type="button" value="Yes"/> <input checked="" type="button" value="No"/>
Are there extenuating circumstances such as: The system provides critical process flow or security capability, the public visibility of the system, the sheer number of other systems reliant on its operation, or the overall cost of the systems replacement?	<input type="button" value="Yes"/> <input checked="" type="button" value="No"/>
Would unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) adversely affect operations or seriously damage mission function and/or public confidence?	<input type="button" value="Yes"/> <input checked="" type="button" value="No"/>
Would either physical or logical destruction of the system result in very large expenditures to restore the system and/or require a long period of time for recovery?	<input type="button" value="Yes"/> <input checked="" type="button" value="No"/>
Does the mission served by the system, or the information that the system processes, affect the security of critical infrastructures and key resources?	<input type="button" value="Yes"/> <input checked="" type="button" value="No"/>
Does the system store, communicate, or process any privacy act information?	<input type="button" value="Yes"/> <input checked="" type="button" value="No"/>
Does the system store, communicate, or process any trade secrets information?	<input type="button" value="Yes"/> <input checked="" type="button" value="No"/>

**Figure: Answer Questions**

After the Answer Questions section is opened, CSET will display a set of eight questions that were taken from the NIST documents. The answers to these questions may cause the SAL values to be changed. As the user marks either Yes or No to the question, CSET will dynamically update the Adjusted for System Questions fields at the top of the screen. The SAL will affect how many questions must be answered in both the Questions and Standard Requirements modes.

**Determine Special Factors:** The final step is to determine the Special Factors. They come from NIST SP800-60, Volume II and are exceptions to the provisional impact assignments of Low, Medium, and High for the selected information type. To add the Special Factors text to the SAL Values, click the security objective value assignment for that information type. Not all information types are associated with Special Factors. Those that are associated with Special Factors have a blue text color (Seen in Figure Checkboxes). Clicking the link will enter that Special Factors text into the field shown Figure. Determine Special Factors.

For example, selecting Air Transportation results in the Confidentiality value of Low, which is seen in blue. Clicking the word Low enters the Special Factor text into the block at the bottom of the screen. This text is fully editable.

**Determine Special Factors**

**Confidentiality Special Factor**

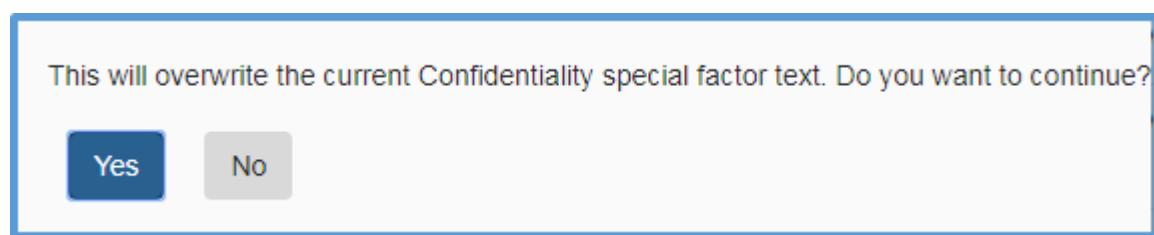
Special Factors Affecting Confidentiality Impact Determination: Unauthorized disclosure of information (e.g., investigations, maintenance) that has not been adequately researched, coordinated, or edited can result in serious economic harm to individuals and to corporations. Loss in public confidence is a further

**Integrity Special Factor**

**Availability Special Factor**

**Figure: Determine Special Factors**

If another information type is checked and the Special Factor text is entered into the block for the same security objective, the previous text in the Special Factors text areas will be overwritten. A warning message, similar to that shown in the Figure below, will be shown to confirm that the text is to be overwritten. Only one Special Factor may be used for each security objective.



**Figure: Special Factors Overwrite Warning**

1

## Overall SAL Widget

Overall	Confidentiality	Integrity	Availability
Very High	Low	Low	Low

The SAL Widget is a display only image that indicates to the user how their SAL selections are affecting the Overall SAL.

2

## NIST/FIPS SAL button

NIST-60 / FIPS-199

The NIST-60/FIPS-199 SAL button is blue when selected. This indicates that the user is on the NIST/FIPS SAL screen.

3

## Overall SAL Selection buttons

Overall SAL

Low   Moderate   High   Very High

The Overall SAL Selection buttons allow the user to quickly and easily select the Overall SAL for the assessment. Simply select the appropriate level and then click the "Next" button to navigate to the next screen. The selected SAL will be saved and associated with the assessment.

The default SAL is Low. The available levels include:

- Low
- Moderate
- High
- Very High

Low, Moderate, and High correspond with the levels identified by NIST in the NIST SP800-53 Standards, the NIST SP800-60 Volumes 1 and 2 documents, and the Chemical Facility Anti-Terrorism Standards (CFATS) risk-based tiering structure. Very High is defined in CSET as comprising all controls including all optional enhancements. It is used to accommodate the multiple Standards available in CSET.

The levels of potential impact are defined as:

**Low:** The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

**Moderate:** The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

**High:** The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

**Very High:** A level of Very High is not defined in the NIST SP800-53 based Standards. It is included in CSET to accommodate the multiple Standards available in the tool and is defined as including all controls and all optional control enhancements.

4

## Confidentiality SAL Selection button

### 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

The Confidentiality SAL Selection buttons allow the user to select the appropriate Confidentiality level if it is known. The overall SAL will be determined based on the highest level selected between the selected Confidentiality, Integrity, and Availability levels.

5

## Integrity SAL Selection button

### Integrity

This value relates to 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.

Low    Moderate    High    Very High

The Integrity SAL Selection buttons allow the user to select the appropriate Integrity level if it is known. The overall SAL will be determined based on the highest level selected between the selected Confidentiality, Integrity, and Availability levels.

6

## Availability SAL Selection button

### Availability

This value relates to the importance of information being readily available. The more important it is to have your information available for use the higher your SAL level.

Low    Moderate    High    Very High

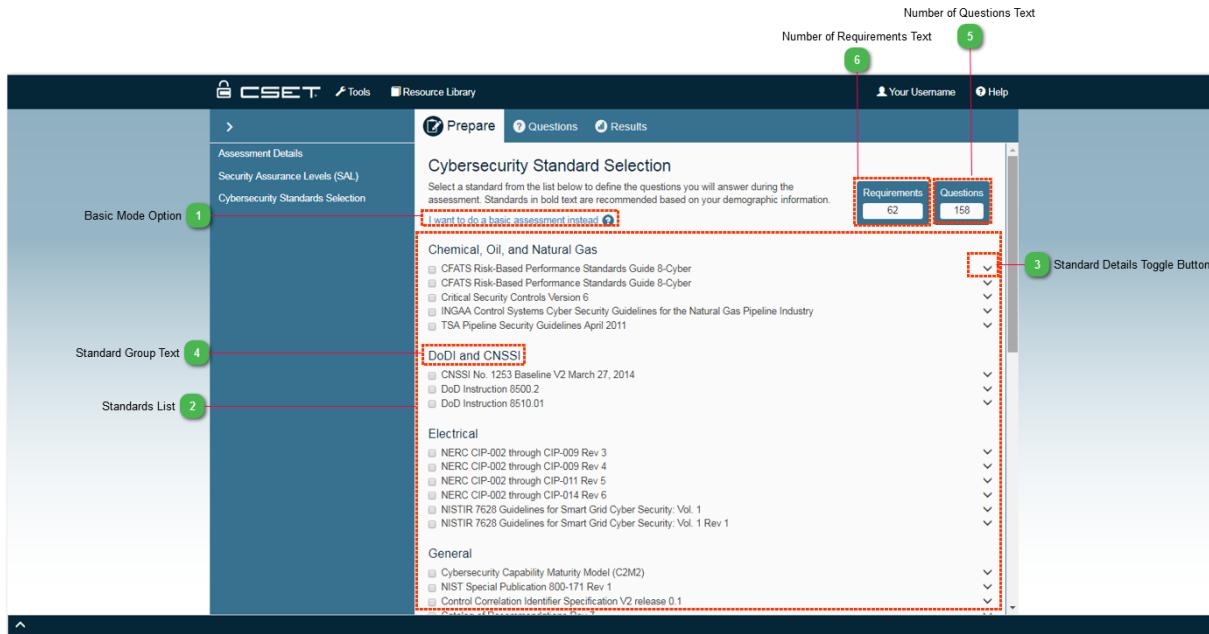
The Availability SAL Selection buttons allow the user to select the appropriate Availability level if it is known. The overall SAL will be determined based on the highest level selected between the selected Confidentiality, Integrity, and Availability levels.

Tip: CSET only uses one of the SAL types. The highest SAL rating out of all of them is what the user's assessment will be based on.

# Cybersecurity Standard Selection

This section provides information on understanding the Standards and requirements available in CSET. The Figure below describes the Cybersecurity Standard Selection screen.

CSET Standards are defined on the [CSET Standards and Groupings](#) page.



**Figure: Cybersecurity Standard Selection Screen**

## 1 Basic Mode Option

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

Selecting the Basic Mode Option will cause the CSET tool to build the assessment questions based on the sector, demographic and other information selected during the preparation process. A knowledge of cybersecurity Standards is not required for the Basic Mode option.

## 2 Standards List

Chemical, Oil, and Natural Gas	
<input type="checkbox"/> CFATS Risk-Based Performance Standards Guide 8-Cyber	▼
<input type="checkbox"/> CFATS Risk-Based Performance Standards Guide 8-Cyber	▼
<input type="checkbox"/> Critical Security Controls Version 6	▼
<input type="checkbox"/> INGAA Control Systems Cyber Security Guidelines for the Natural Gas Pipeline Industry	▼
<input type="checkbox"/> TSA Pipeline Security Guidelines April 2011	▼
DoDI and CNSSI	
<input type="checkbox"/> CNSSI No. 1253 Baseline V2 March 27, 2014	▼
<input type="checkbox"/> DoD Instruction 8500.2	▼
<input type="checkbox"/> DoD Instruction 8510.01	▼
Electrical	
<input type="checkbox"/> NERC CIP-002 through CIP-009 Rev 3	▼
<input type="checkbox"/> NERC CIP-002 through CIP-009 Rev 4	▼
<input type="checkbox"/> NERC CIP-002 through CIP-011 Rev 5	▼
<input type="checkbox"/> NERC CIP-002 through CIP-014 Rev 6	▼
<input type="checkbox"/> NISTIR 7628 Guidelines for Smart Grid Cyber Security: Vol. 1	▼
<input type="checkbox"/> NISTIR 7628 Guidelines for Smart Grid Cyber Security: Vol. 1 Rev 1	▼
General	
<input type="checkbox"/> Cybersecurity Capability Maturity Model (C2M2)	▼
<input type="checkbox"/> NIST Special Publication 800-171 Rev 1	▼
<input type="checkbox"/> Control Correlation Identifier Specification V2 release 0.1	▼

The Standards List displays a list of all available Standards on which the assessment questions may be based. Some standards will be recommended based on demographic information indicated by the user (shown in bold). Some Standards are only available in "Requirements Mode" and may be disabled based on the assessment mode previously selected. Standards are organized into Groups and can be sorted accordingly. Each Standard also has details or descriptions to help the user better identify the Standard.

Any Custom Questionnaires associated with the installation of CSET will also be available on the Standard List.

This is where the unlocked Standards from [Enable Protected Features](#) will be shown.

3

## Standard Details Toggle Button

The Standard Details toggle button will toggle between showing and hiding descriptions of the selected Standard to help the user better understand what the Standards contain.

4

## Standard Group Text

### DoDI and CNSSI

The Standard Group text shows the group to which a specific Standard belongs. The Standard List is sorted by the Group to help the user more easily find specific Standards within a group.

5

## Number of Questions Text



The Number of Questions Text will update as Standards are selected and provides an indication to the user how large the assessment will be.

6

## Number of Requirements Text



The Number of Requirements Text will update as Standards are selected and provides an indication to the user how large the assessment will be.

## CSET Standards and Groupings

This page describes the Cybersecurity Standards used by the CSET tool. Standards are grouped into multiple areas as explained below.

### Chemical, Oil, and Natural Gas

**Critical Security Controls Version 6:** The Center for Internet Security (CIS) presents the CIS Controls for Effective Cyber Defense Version 6.0, a recommended set of actions that provide specific and actionable ways to stop today's most pervasive and dangerous cyber attacks. The CIS Controls are especially relevant because they are updated by cyber experts based on actual attack data pulled from a variety of public and private threat sources. Version 6 incorporates recommended changes from the cybersecurity community to reflect the latest technologies and threats. The new Controls include a new Control for "Email and Web Browser Protections," a deleted Control on "Secure Network Engineering," and a re-ordering to make "Controlled Use of Administration Privileges" higher in priority. This version also includes a new metrics companion guide.

**CFATS Risk-Based Performance Standards Guide 8—Cyber:** This Standards guidance is part of the overall efforts defined in 6 Code of Federal Regulations (CFR) Part 27 to protect chemical facilities from the effects of a terrorist attack. CFATS, or the Chemical Facilities Anti-Terrorism Standards, is made up of 18 Risk-Based Performance Standards Guidance (RBPS) sections that provide guidance on protecting various aspects of a chemical facility. RBPS 8 is focused on cybersecurity with emphasis on protecting both information management and control system-based networks. It is the only RBPS that is pertinent to the CSET.

The audience for this instruction is personnel involved in the chemical industry who are required to comply with the 6 CFR Part 27 as well as others seeking to follow these simple actions to better protect their systems.

DHS has developed a risk-based tiering structure that will allow it to focus resources on the high-risk chemical facilities. To that end, DHS will assign facilities to one of four risk-based tiers ranging from very high (Tier 1) to low (Tier 4) risk. These tiers are unrelated to the Framework tiers.

### **INGAA Control Systems Cyber Security Guidelines for the Gas**

**Pipeline Industry:** The Interstate Natural Gas Association of America (INGAA) is a trade organization for the natural gas pipeline industry in North America. As such, its Standard applies to the gas pipeline industry. The guidelines can be thought of as a subset of the Transportation Security Administration (TSA) Pipeline Security Guidelines and focus on securing large supervisory control and data acquisition (SCADA) systems and smaller, local control systems. The intended audience is administrators, network security personnel, SCADA software manufacturers, operators, vendors, and other stakeholders involved in the natural gas pipeline industry. Because INGAA is a non-government body, a disclaimer will be seen upon selection of this Standard.

**TSA Pipeline Security Guidelines, April 2011:** This Transportation Security Administration (TSA) document provides a set of short guidelines for protecting and securing the transportation of various liquids through transmission pipelines. It includes cybersecurity guidelines in addition to other security measures including physical protection, personnel security, equipment maintenance and testing, etc. These guidelines are applicable to natural gas and hazardous liquid transmission pipelines, natural gas distribution pipelines, and to liquefied natural gas facility operators. In addition, these guidelines apply to pipeline systems that transport material categorized as toxic inhalation hazards (TIHs).

## DODI and CNSSI:

**CNSSI No. 1253 Baseline, V2 March 27, 2014:** This update was released in March of 2014 and supersedes the older CNSSI No. 1253 Baseline listed earlier. The intent and purpose of the Standard is the same as described above. Use this version for new assessments.

**DoD Instruction 8500.2:** This DoD Instruction, Information Assurance (IA) Implementation, implements policy, assigns responsibilities, and prescribes procedures for applying integrated, layered protection to DoD information systems and networks. It is applicable to information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of U.S. military-related information. It is predicated on five competencies, the ability to: (1) assess security needs and capabilities, (2) develop a purposeful security design or configuration, (3) implement required controls or safeguards, (4) test and verify, and (5) manage changes to an established baseline in a secure manner. The audience for this instruction is personnel who use IT to share DoD information across the Global Information Grid.

**DoD Instruction 8510.01:** Risk Management Framework (RMF) for DoD IT applies to all DoD IT that receives, processes, stores, displays, or transmits DoD information. The instruction implements NIST SP 800-37 and re-designates the DIACAP Technical Advisory Group (TAG) as the RMF TAG. The instruction also provides procedural guidance for the reciprocal acceptance of authorization decisions and artifacts within DoD, and between DoD and other federal agencies, for the authorization and connection of information systems. It uses controls from CNSSI 1253 V2 plus NIST SP800-53 Appendix J.

## Electrical:

**NERC CIP-002 through CIP-009, Rev. 3:** The North American Electric Reliability Council (NERC) Critical Infrastructure Protection (CIP) Standards apply to the electric power industry. Standards CIP-002 through CIP-009 provide a cybersecurity framework (unrelated to the cybersecurity framework based Assessment Mode option) for the identification and protection of critical cyber assets to support reliable operation of the bulk electric system.

Standard CIP-002-3 requires the identification and documentation of the critical cyber assets. Standard CIP-003-3 requires that responsible entities have minimum security management

controls in place to protect critical cyber assets. Standard CIP-004-3 requires that personnel having authorized cyber or authorized unescorted physical access to critical cyber assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. Standard CIP-005-3 requires the identification and protection of the electronic security perimeters. Standard CIP-006-3 is intended to ensure the implementation of a physical security program. Standard CIP-007-3 requires responsible entities to define methods, processes, and procedures for securing those systems determined to be critical cyber assets. Standard CIP-008-3 ensures the identification, classification, response, and reporting of cybersecurity incidents; and Standard CIP-009-3 ensures that recovery plans are put in place.

The NERC CIP Standards are designed specifically for the needs of the electric power sector.

**NERC CIP-002 through CIP-009, Rev. 4:** Revision 4 of the CIP Standards has the same aims and audience as Revision 3. This version includes all the requirements that have been added or modified for Revision 4.

**NERC CIP-002 through CIP-011, Rev. 5:** Revision 5 of the CIP Standards has the same aims and audience as Versions 3 and 4. It does, however, include two additional sections. CIP-010 deals with configuration change management and vulnerability assessments. CIP-011 is concerned with information protection. This version includes all the requirements that have been added or modified for Revision 5.

**NERC CIP-002 through CIP-011, Rev. 6:** NERC CIP v6 is largely about scope, and so its impact will be dependent on how the scope expansion affects your organization. The expansion of requirements to low impact assets has zero impact if you don't have any. The same goes for the transient assets and removable media. While there aren't many organizations in that situation, scope reduction is absolutely a valid strategy for any compliance program, NERC CIP compliance included. While it may seem obvious to state, don't wait to determine how you're going to address the updated NERC CIP standards. If there's the potential for budgetary impact (and there is), the sooner you start planning, the better.

### **NISTIR 7628 Guidelines for Smart Grid Cyber Security, Vol 1:**

Dealing with Standards for the national electrical transmission systems and applicable to the electric sector, this National Institute of Standards and Technology (NIST) Interagency Report (IR) presents a framework that organizations can use to develop cybersecurity strategies to secure existing systems while upgrading to newer, smart grid technology. NISTIR includes identification of security requirements, risk assessment processes, and high-level architecture. It presents a sample logical interface reference model used to identify and define 22 logical interface categories within and across seven commonly accepted Smart Grid domains. The intended audience is individuals and organizations responsible for addressing cybersecurity for Smart Grid systems and the constituent subsystems of hardware and software components.

### **NISTIR 7628 Guidelines for Smart Grid Cyber Security, Vol 1 Rev. 1:**

Revision 1 of the NISTIR 7628 Guideline has the same aims and audience as the earlier version, but with updated information on Smart Grid technologies and implementations.

## **General:**

**Catalog of Recommendations, Rev. 7:** The Catalog of Recommendations or CoR questionnaires are based on the Catalog of Control Systems Security, Recommendations for Standards Developers. Development was initially sponsored by DHS with input from NIST and five national laboratories. Its original intent was to serve as a source of requirements and controls for the developers of ICS Standards. The CoR consolidated the requirements from 15 control system and information technology Standards. Version 7 is the latest version and incorporates changes and updates made in 2010.

The controls in the CoR are organized into families based on NIST SP800-53 with contributions from AGA, ISO, IEC, IEEE, ISA, NERC, and other Standards documents. Requirements for each security control include: (1) detailed recommended security practices and mechanisms, (2) supplemental guidance with information that may be beneficial for understanding and implementing the recommendations, and (3) requirement enhancements including supplementary security constraints for the recommendations.

The CoR is not limited for use by a specific industry sector. It is intended to be broad enough to provide any industry using control systems the flexibility needed to develop sound cybersecurity Standards specific to their individual security needs. Its use is strongly recommended if using the Standards-based approach.

**Control Correlation Identifier Specification V2 release 0.1:** One of the more recent information security innovations is the Control Correlation Identifier, or CCI. Each CCI

provides a standard identifier and description for “singular, actionable statements” that comprise a security control or security best practice. The purpose of CCIs is to allow a high level statement made in a policy document (i.e., a security control) to be “decomposed” and explicitly associated with the low-level security settings that must be assessed to determine compliance with the objectives of that specific statement. Under the leadership of the Defense Information Systems Agency (DISA), a working group has been cataloging CCIs for the past several years. The collection has now been developed to the point that every assessment objective in the NIST SP 800-53A has been mapped to an individual CCI. The current list of CCIs can be downloaded in XML format (viewable in a web browser such as Internet Explorer). The URL for downloading is: <http://iase.disa.mil/stigs/cci/Pages/index.aspx>. DISA encourages feedback from the information security community; a comment form is provided for that purpose. DISA is also in the process of revising numerous Security Technical Implementation Guides (STIGs) to include references to CCIs that correspond to each of the recommended configuration settings.

**Cybersecurity Capability Maturity Model (C2M2)**: The C2M2 is designed to be used by any organization to enhance its own cybersecurity capabilities. It focuses on the implementation and management of cybersecurity practices associated with the operation and use of information technology and operational technology assets and the environments in which they operate. The goal is to measure the maturity of an organization’s cybersecurity capabilities and support ongoing development within an organization. To do so, it uses a system of Maturity Indicator Levels (MILs) applied to each of ten key domains such as Risk Management and Configuration Management.

MIL 0 is the lowest of the maturity models and is defined as Incomplete. Many organizations can achieve MIL 0 using an ad hoc approach. MIL 1 is Initiated, MIL 2 is Performed, and MIL 3, the highest maturity level, is Managed.

Also available are sector-specific C2M2s for Electricity, and Oil and Natural Gas that include the core C2M2 as well as additional reference material and implementation guidance specifically tailored for the referenced sector.

**NIST Special Publication 800-171**: This publication provides federal agencies with recommended requirements for protecting the confidentiality of Controlled Unclassified Information (CUI): (i) when the CUI is resident in nonfederal information systems and organizations; (ii) when the information systems where the CUI resides are not used or operated by contractors of federal agencies or other organizations on behalf of those agencies; and (iii) where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or government-wide policy for the CUI category or subcategory listed in the CUI Registry. The requirements apply to all components of nonfederal information systems and organizations that process, store, or transmit CUI, or provide security protection for such components.

**NIST Special Publication 800-171 Rev. 1**: The protection of Controlled Unclassified Information (CUI) resident in nonfederal systems and organizations is of paramount importance to federal agencies and can directly impact the ability of the federal government to successfully conduct its assigned missions and business operations. This publication provides federal agencies with a set of recommended security requirements for protecting the confidentiality of CUI when such information is resident in nonfederal systems and organizations; when the nonfederal organization is not collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency; and where

there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or governmentwide policy for the CUI category or subcategory listed in the CUI Registry. The security requirements apply to all components of nonfederal systems and organizations that process, store, or transmit CUI, or that provide security protection for such components. The requirements are intended for use by federal agencies in contractual vehicles or other agreements established between those agencies and nonfederal organizations.

### **Payment Card Industry (PCI) Data Security Standard:**

The Payment Card Industry Data Security Standard (PCI DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect account data. PCI DSS applies to all entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers. PCI DSS also applies to all other entities that store, process or transmit cardholder data (CHD) and/or sensitive authentication data (SAD).

## **Health Care**

### **Health Insurance Portability and Accountability Act Security Rule:**

The Health Insurance Portability and Accountability Act of 1996 (HIPAA; Pub.L. 104-191, 110 Stat. 1936, enacted August 21, 1996) was enacted by the United States Congress and signed by President Bill Clinton in 1996. It has been known as the Kennedy–Kassebaum Act or Kassebaum–Kennedy Act after two of its leading sponsors.<sup>[1][2]</sup> Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs. Title II of HIPAA, known as the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers. Technical Safeguards – controlling access to computer systems and enabling covered entities to protect communications containing PHI transmitted electronically over open networks from being intercepted by anyone other than the intended recipient. Information systems housing PHI must be protected from intrusion. When information flows over open networks, some form of encryption must be used. If closed systems or networks are used, existing access controls are considered sufficient and encryption is optional. Each covered entity is responsible for ensuring that the data within its systems have not been changed or erased in an unauthorized manner. Data corroboration, including the use of check sum, double-keying, message authentication, and digital signature may be used to ensure data integrity. Covered entities must also authenticate entities with which they communicate. Authentication consists of corroborating that an entity is who it claims to be. Examples of corroboration include: password systems, two or three-way handshakes, telephone callback, and token systems. Covered entities must make documentation of their HIPAA practices available to the government to determine compliance. In addition to policies and procedures and access records, information technology documentation should also include a written record of all configuration settings on the components of the network because these components are complex, configurable, and always changing. Documented risk analysis and risk management programs are required. Covered entities must carefully consider the risks of their operations as they implement systems to comply with the act. (The requirement of risk analysis and risk management implies that the act's security requirements are a minimum standard and places responsibility on covered entities to take all reasonable precautions necessary to prevent PHI from being used for non health purposes.)

## Information Technology:

The National Institute of Standards and Technology (NIST), Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems and Organizations, is the primary U.S. government Standard for securing information systems. Because many non federal entities have adopted its use, it is probably the most widely used Standard for IT system security.

**NIST Special Publication 800-53, Rev. 3:** The NIST SP800-53 provides guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the U.S. federal government. The guidelines apply to all components of an information system that process, store, or transmit federal information. Information system components can include mainframes, servers, workstations, operating systems, and applications. Network components can include firewalls, switches, routers, wireless access points, and network appliances. Servers can include database servers, authentication servers, electronic mail and web servers, proxy servers, and domain name servers. Information system components may be purchased commercially off-the-shelf or custom developed.

Although developed for the federal government, other organizations are encouraged to use the guidelines. In CSET, this version of the Standard does not include the adjustments addressed in Appendix I. See NIST SP800-53, Rev. 3 with Appendix I for those modified controls.

**NIST Special Publication 800-53, Rev. 4:** Revision 4 has the same audience and intended use as Revision 3; however, it includes updates, additions, and changes to make it more current and relevant. In CSET, Appendix I is separate.

**NIST Special Publication 800-53, Rev. 4 App J:** Appendix J of 800-53, Rev. 4, is titled the Privacy Control Catalog. It relates specifically to protection of individuals' privacy and their personally identifiable information (PII). The appendix provides a structured set of controls for protecting privacy and serves as a roadmap for organizations to use in identifying and implementing privacy controls concerning the entire life cycle of PII.

## Supply Chain:

**Framework for Improving Critical Infrastructure Cybersecurity 1.1:** The Framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes. The Framework consists of three parts: the Framework Core, the Implementation Tiers, and the Framework Profiles. The Framework Core is a set of cybersecurity activities, outcomes, and informative references that are common across sectors and critical infrastructure. Elements of the Core provide detailed guidance for developing individual organizational Profiles. Through use of Profiles, the Framework will help an organization to align and prioritize its cybersecurity activities with its business/mission requirements, risk tolerances, and resources. The Tiers provide a mechanism for organizations to view and understand the characteristics of their approach to managing cybersecurity risk, which will help in prioritizing and achieving cybersecurity objectives.

## Nuclear:

### **NEI 08-09 Cyber Security Plan for Nuclear Power Reactors:**

The Nuclear Energy Institute (NEI) developed this Standard to assist nuclear energy facilities in meeting cybersecurity regulations required by 10 CFR 73.54 and the NRC. NEI 08-09 describes a defensive strategy that consists of a defensive architecture and set of security controls that is based on NIST SP 800-82 and NIST SP 800-53. Because INGAA is a nongovernment body, a disclaimer will be seen upon selection of this Standard.

**NRC Regulatory Guide 5.71:** The Nuclear Regulatory Commission, Regulatory Guide 5.71 (NRC RG 5.71), Cyber Security Programs for Nuclear Facilities, provides a framework to aid in the identification of those digital assets, referred to as critical digital assets or CDAs, which must be protected from cyber attacks. The framework offers licensees and applicants the ability to address the specific needs of an existing or new system. Thus the framework provides a flexible programmatic approach in which the licensee or applicant can establish, maintain, and successfully integrate security controls into a site-specific cybersecurity program. The intended audience is owners and operators of nuclear power plants.

## Process Control and SCADA:

**NIST Special Publication 800-53, Rev. 3 with App I:** Appendix I of the NIST SP800-53 adds guidance on industrial control system (ICS) security to the control system guidance already contained in the publication. In this context, an ICS is an information system used to control industrial processes such as manufacturing, product handling, production, and distribution. ICSs include supervisory control and data acquisition (SCADA) systems, distributed control systems (DCSs), and programmable logic controllers (PLCs). The appendix modifies selected questions and requirements in SP800-53 based on the differences between ICS and typical information systems.

The information in Appendix I is not as comprehensive as that found in NIST SP800-82, but may provide useful information on tailoring, security controls, and control enhancements. NIST guidance was developed for the federal government, but other organizations are encouraged to use it.

**NIST Special Publication 800-82:** The NIST Guide to Industrial Control Systems (ICS) Security publication provides guidance for establishing a secure ICS including SCADA systems, DCSs, and other systems performing control functions. It identifies typical threats and vulnerabilities to these systems, provides recommended security countermeasures to mitigate the associated risks, and includes a list of many different methods and techniques for securing ICSs.

The scope includes ICSs that are typically used in the electric, water, oil and gas, chemical, pharmaceutical, pulp and paper, food and beverage, and discrete manufacturing (automotive, aerospace, and durable goods) industries. This version of SP800-82 is based on the formal publication of the document in June 2011.

**NIST Special Publication 800-82, Rev. 1:** Revision 1 of the NIST SP 800-82

Standard has the same aims and audience as the earlier version. This revision includes the integration of the ICS material transferred from Special Publication 800-53, Revision 3.

**NIST Special Publication 800-82, Rev. 2:** Revision 2 of the NIST SP 800-82

Standard has the same aims and audience as the earlier version. This revision includes updates to ICS threats and vulnerabilities, ICS security, ICS risk management, and security capabilities and tools for ICS. It also introduces overlays and provides an ICS overlay for NIST SP 800-53, Revision 4 security controls for tailored security control baselines for Low, Moderate, and High impact ICS.

## Supply Chain

**NIST SP800-161 Supply Chain Risk Management:** Federal agencies are concerned about the risks associated with information and communications technology (ICT) products and services that may contain potentially malicious functionality, are counterfeit, or are vulnerable due to poor manufacturing and development practices within the ICT supply chain. These risks are associated with the federal agencies' decreased visibility into, understanding of, and control over how the technology that they acquire is developed, integrated and deployed, as well as the processes, procedures, and practices used to ensure the integrity, security, resilience, and quality of the products and services. This publication provides guidance to federal agencies on identifying, assessing, and mitigating ICT supply chain risks at all levels of their organizations. The publication integrates ICT supply chain risk management (SCRM) into federal agency risk management activities by applying a multitiered, SCRM-specific approach, including guidance on assessing supply chain risk and applying mitigation activities.

## Transportation

**Defining a Security Zone Architecture for Rail Transit and Protecting**

**Critical Zones:** This Recommended Practice is Part-II in a series of documents to be released. Part-I released in July 2010 addresses the importance of control and communications security to a transit agency, provides a survey of the various systems that constitute typical transit control and communication systems, identifies the steps that an agency would follow to set up a successful program, and establishes the stages in conducting a risk assessment and managing risk. Part-II presents Defense-In-Depth as a recommended approach for securing rail communications and control systems, defines security zone classifications, and defines a minimum set of security controls for the most critical zones, the, SAFETY CRITICAL SECURITY ZONE (SCSZ) and the FIRE, LIFE-SAFETY SECURITY ZONE (FLSZ). Later parts will cover recommended practices for less critical zones, the rail vehicles, and provide other guidance for a transit agency.

The purpose of this Recommended Practice is to share transit agency best practices; set a minimum requirement for control security within the transit industry; provide a guide of common security requirements to control and operations systems vendors; adopt voluntary industry practices in control security in advance and in coordination with government regulation; and raise awareness of control security concerns and issues in the industry.

## Questions Only:

**Key Questions**: The Key Questions are a subset of the Catalog of Recommendations and are limited in scope to what subject matter experts consider to be the top set of requirements. They are geared toward providing meaningful results in a limited amount of time. They should be used only when an assessment based on one or more full Standards cannot be completed within an allotted time. They are intended for any industry using control systems.

**Universal Questions**: The Universal Questions are based on the Catalog of Recommendations and include a full range of ICS security questions. The questions are written as simple, Yes or No questions and are grouped in a set of common security categories. The Universal Questions are the core set of questions found in CSET and should be included with any questions based assessment.

## C2M2 Maturity Indicator Levels

The Cybersecurity Capability Maturity Model (C2M2) Standard uses a system of Maturity Indicator Levels (MILs). They are defined as:

- MIL0: Incomplete
- MIL1: Initiated
- MIL2: Performed
- MIL3: Managed.

They correspond to CSET SALs as follows:

- MIL1: Low
- MIL2: Moderate
- MIL3: High

MIL0 is not used.

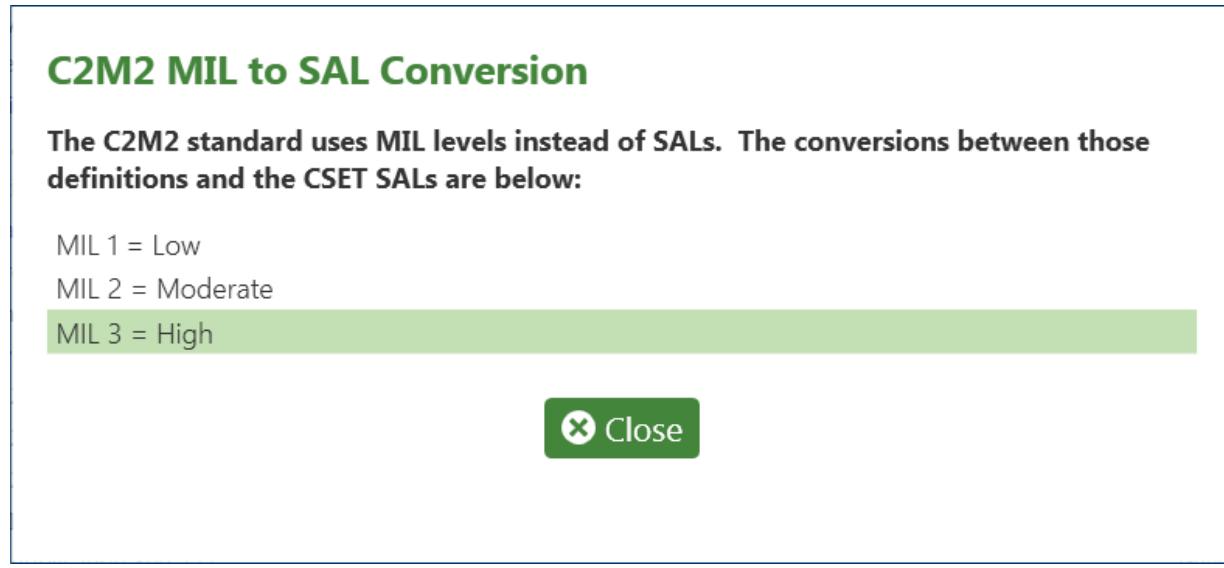
Figure 59 shows the MIL to SAL link next to the C2M2 Standard name on the Cybersecurity Standard Selection screen. Clicking this link opens the C2M2 MIL to SAL Conversion window shown in Figure 60 which shows the MIL to SAL mappings.

When selecting the C2M2 Standard, the user should verify that the selected SAL for the assessment corresponds to the desired MIL.

Cybersecurity Capability Maturity Model (C2M2) [MIL to SAL](#)

General Details ▾

**Figure 59 C2M2 MIL to SAL link**



**Figure 60. C2M2 MIL to SAL Conversion Window**

## CFATS Tiers

The Chemical Facilities Anti-Terrorism Standards (CFATS) Risk-Based Performance Standards Guide 8-Cyber uses Tiers rather than Standard Security Assurance Levels (SALs). To map the CFATS tiers to the SAL options, use the tier designations below.

- Tier I, Very High,
- Tier II, High,
- Tier III, Moderate, and
- Tier IV, Low.

This mapping is reflected on the SAL screen. The CFATS tiers are unrelated to those associated with the Cybersecurity Framework.

Figure 61 shows the Tier to SAL link next to the CFATS Standard name on the Cybersecurity Standard Selection screen. Clicking this link opens the CFATS Tier to SAL Conversion window shown in Figure 62 which shows the Tier to SAL mappings.

When selecting the CFATS Standard, the user should verify that the selected Security Assurance Level (SAL) for the assessment corresponds to the desired Tier.

CFATS Risk-Based Performance Standards Guide 8-Cyber [Tier to SAL](#)

Chemical, Oil, and Natural Gas [Details ▾](#)

**Figure 61. CFATS Tier to SAL Link**

### CFATS Tier to SAL Conversion

**The CFATS standard uses Tier levels instead of SALs. The conversions between those definitions and the CSET SALs are below:**

Tier I = Very High

Tier II = High

Tier III = Moderate

Tier IV = Low

 Close

**Figure 62. CFATS Tier to SAL Conversion Window**

# Cybersecurity Framework Description

This section provides additional information about the Cybersecurity Framework assessment mode. This function was added to CSET in response to Executive Order 13636, Improving Critical Infrastructure Cybersecurity issued on February 12, 2013, which calls for the development of a voluntary risk-based Cybersecurity Framework. The Framework consists of three parts: (1) the Framework Core, (2) the Framework Implementation Tiers, and (3) the Framework Profile.

## Framework Core

The Framework Core is a set of cybersecurity activities and references that are common across critical infrastructure sectors organized around particular outcomes. The Core presents Standards and best practices in a manner that allows for communication of cybersecurity risk across the organization from the senior executive level to the implementation/operations level. The Framework Core consists of five functions - Identify, Protect, Detect, Respond, Recover that can provide a high-level, strategic view of an organization's management of cybersecurity risk.

The functions are described as follows:

**Identify.** Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.

**Protect.** Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.

**Detect.** Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.

**Respond.** Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.

**Recover.** Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

The Framework Core then identifies underlying key Categories and Subcategories for each of these functions and matches them with example Informative References such as existing Standards, guidelines, and practices for each Subcategory. This structure ties the high level strategic view, outcomes, and Standards-based actions together for a cross-organization view of cybersecurity activities.

The Framework stems from the principle of common criteria. Common criteria processes are particularly useful as a driving force for the mutual recognition and adoption of secure IT products. By using a common criteria framework, users can develop a common understanding of their security requirements (their protection profile) and communicate these to vendors, business partners, and sector associations.

The Functions and Categories are identified as shown in the Figure below.

Function Unique Identifier	Function	Category Unique Identifier	Category Name
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

**Figure: Function and Category Identifiers**

The Framework Core represents a common set of activities for managing cybersecurity risk. In other words, it presents what owners and operators of cyber assets should do to secure their systems. While it is not exhaustive, it is extensible, allowing organizations, sectors, and other entities to use Subcategories and Informative References that are cost-effective and efficient and that enable the organizations to manage their cybersecurity risk.

As an example, the recommended activities for Asset Management are shown in the Figure below. The actions listed under Subcategory will, when implemented, increase cybersecurity and decrease risk. The provided references are the Standards and guidelines from whence the recommended actions were derived.

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	Asset Management (AM): The personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	ID.AM-1: Physical devices and systems within the organization are inventoried	<ul style="list-style-type: none"> <li>• ISA 99.02.01 4.2.3.4</li> <li>• COBIT BAI03.04, BAI09.01, BAI09, BAI09.05</li> <li>• ISO/IEC 27001 A.7.1.1, A.7.1.2</li> <li>• NIST SP 800-53 Rev. 4 CM-8</li> <li>• CCS CSC1</li> </ul>
		ID.AM-2: Software platforms and applications within the organization are inventoried	<ul style="list-style-type: none"> <li>• ISA 99.02.01 4.2.3.4</li> <li>• COBIT BAI03.04, BAI09.01, BAI09, BAI09.05</li> <li>• ISO/IEC 27001 A.7.1.1, A.7.1.2</li> <li>• NIST SP 800-53 Rev. 4 CM-8</li> <li>• CCS CSC 2</li> </ul>
		ID.AM-3: The organizational communication and data flow is mapped	<ul style="list-style-type: none"> <li>• ISA 99.02.01 4.2.3.4</li> <li>• COBIT DSS05.02</li> <li>• ISO/IEC 27001 A.7.1.1</li> <li>• NIST SP 800-53 Rev. 4 CA-3, CM-8, CA-9</li> <li>• CCS CSC 1</li> </ul>
		ID.AM-4: External information systems are catalogued	<ul style="list-style-type: none"> <li>• COBIT 5 APO02.02</li> <li>• ISO/IEC 27001:2013 A.11.2.6</li> <li>• NIST SP 800-53 Rev. 4 AC-20, SA-9</li> </ul>
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	<ul style="list-style-type: none"> <li>• COBIT 5 APO03.03, APO03.04, BAI09.02</li> <li>• ISA 62443-2-1:2009 4.2.3.6</li> <li>• ISO/IEC 27001:2013 A.8.2.1</li> <li>• NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14</li> </ul>
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	<ul style="list-style-type: none"> <li>• COBIT 5 APO01.02, DSS06.03</li> <li>• ISA 62443-2-1:2009 4.3.2.3.3</li> <li>• ISO/IEC 27001:2013 A.6.1.1</li> <li>• NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11</li> </ul>

**Figure: Framework Core Example**

## Framework Tiers

Framework Implementation Tiers (Tiers) provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. The Tier selection process considers an organization's current risk management practices, threat environment, legal and regulatory requirements, business/mission objectives, and organizational constraints. The Tiers characterize an organization's practices over a range, from Partial (Tier 1) to Adaptive (Tier 4), progressing from informal, reactive implementations to approaches that are agile and risk-informed.

The Figure below lists the risk categories and tier levels. A tier is applied to each of the risk categories. The tiers are described below and presented in relation to each category.

Risk Categories	Tiers
Risk Management Process	Tier 1: Partial
Integrated Risk Management Program	Tier 2: Risk Informed
External Participation	Tier 3: Repeatable
	Tier 4: Adaptive

**Figure: Risk Categories and Tiers**

### **Tier 1: Partial**

- **Risk Management Process** – Organizational cybersecurity risk management practices are not formalized, and risk is managed in an ad hoc and sometimes reactive manner. Prioritization of cybersecurity activities may not be directly informed by organizational risk objectives, the threat environment, or business/mission requirements.
- **Integrated Risk Management Program** – Awareness of cybersecurity risk is limited at the organizational level, and an organization-wide approach to managing cybersecurity risk has not been established. The organization implements cybersecurity risk management on an irregular, case-by-case basis because of varied experience or information gained from outside sources. The organization may not have processes that enable cybersecurity information to be shared within the organization.
- **External Participation** – An organization may not have the processes in place to participate in coordination or collaboration with other entities.

### **Tier 2: Risk Informed**

- **Risk Management Process** – Risk management practices are approved by management but may not be established as an organization wide policy. Prioritization of cybersecurity activities is directly informed by organizational risk objectives, the threat environment, or business/mission requirements.
- **Integrated Risk Management Program** – There is an awareness of cybersecurity risk at the organizational level, but an organization-wide approach to managing cybersecurity risk has not been established. Risk-informed, management-approved processes and procedures are defined and implemented, and staff has adequate resources to perform their cybersecurity duties. Cybersecurity information is shared within the organization on an informal basis.

- **External Participation** – The organization knows its role in the larger ecosystem, but has not formalized its capabilities to interact and share information externally.

### Tier 3: Repeatable

- **Risk Management Process** – The organization's risk management practices are formally approved and expressed as policy. Organizational cybersecurity practices are regularly updated based on the application of risk management processes to changes in business/mission requirements and a changing threat and technology landscape.
- **Integrated Risk Management Program** – There is an organization-wide approach to manage cybersecurity risk. Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed. Consistent methods are in place to respond effectively to changes in risk. Personnel possess the knowledge and skills to perform their appointed roles and responsibilities.
- **External Participation** – The organization understands its dependencies and partners and receives information from these partners that enables collaboration and risk-based management decisions within the organization in response to events.

### Tier 4: Adaptive

- **Risk Management Process** – The organization adapts its cybersecurity practices based on lessons learned and predictive indicators derived from previous and current cybersecurity activities. Through a process of continuous improvement incorporating advanced cybersecurity technologies and practices, the organization actively adapts to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a timely manner.
- **Integrated Risk Management Program** – An organization-wide approach to managing cybersecurity risk uses risk-informed policies, processes, and procedures to address potential cybersecurity events. Cybersecurity risk management is part of the organizational culture and evolves from an awareness of previous activities, information shared by other sources, and continuous awareness of activities on their systems and networks.
- **External Participation** – The organization manages risk and actively shares information with partners to ensure that accurate, current information is being distributed and consumed to improve cybersecurity before a cybersecurity event occurs.

Successful implementation of the Framework is based on achievement of the outcomes described in the organization's Target Profiles and not on Tier determination.

## Framework Profiles

The Framework Profile (Profile) is the alignment of the Functions, Categories, and Subcategories with the business requirements, risk tolerance, and resources of the organization. A profile enables organizations to establish a roadmap for reducing cybersecurity

risk that is well aligned with organizational and sector goals, considers legal/regulatory requirements and industry best practices, and reflects risk management priorities. Given the complexity of many organizations, they may choose to have multiple profiles, aligned with particular components and recognizing their individual needs.

Framework Profiles can be used to describe the current state or the desired target state of specific cybersecurity activities. They support business/mission requirements and aid in the communication of risk within and between organizations. They can reveal gaps to be addressed to meet cybersecurity risk management objectives. Profiles can be used to conduct self-assessments and communicate requirements and results within an organization or between organizations.

# Framework Implementation Tiers

If Cybersecurity Framework is selected as the assessment mode, the screen will allow for assignment of the framework tiers. Framework tiers are not related to the CFATS tiers. The Figure below shows the screen when Cybersecurity Framework-based and the Implementation Tiers tab are selected.

**Figure: Framework Implementation Tiers Screen**

1

## Implementation Tier List

### Cybersecurity Framework

Select the cybersecurity framework profile you want to use for your assessment. The baseline cybersecurity framework profile comes preloaded with CSET that you can copy to get started when creating your own custom profiles. You can also create a new custom profile or update and export existing profiles.

#### External Participation

- Tier 1**  
An organization may not have the processes in place to participate in coordination or collaboration with other entities.
- Tier 2**  
The organization knows its role in the larger ecosystem, but has not formalized its capabilities to interact and share information externally.
- Tier 3**  
The organization understands its dependencies and partners and receives information from these partners that enables collaboration and risk-based management decisions within the organization in response to events.
- Tier 4**  
The organization manages risk and actively shares information with partners to ensure that accurate, current information is being distributed and consumed to improve cybersecurity before a cybersecurity event occurs.

#### Integrated Risk Management Program

- Tier 1**  
There is limited awareness of cybersecurity risk at the organizational level and an organization-wide approach to managing cybersecurity risk has not been established. The organization implements cybersecurity risk management on an irregular, case-by-case basis due to varied experience or information gained from outside sources. The organization may not have processes that enable cybersecurity information to be shared within the organization.
- Tier 2**  
There is an awareness of cybersecurity risk at the organizational level but an organization-wide approach to managing cybersecurity risk has not been established. Risk-informed, management-approved processes and procedures are defined

The Implementation Tier list indicates the framework tier level for the selected risk category. Users should select the tier that most accurately describes their organization.

## Mode Selection

Mode Selection is available at the top of the Questions/Requirements page and allows the user to determine the general approach they want to take with completing the assessment. The Figure below describes the Mode Selection screen.

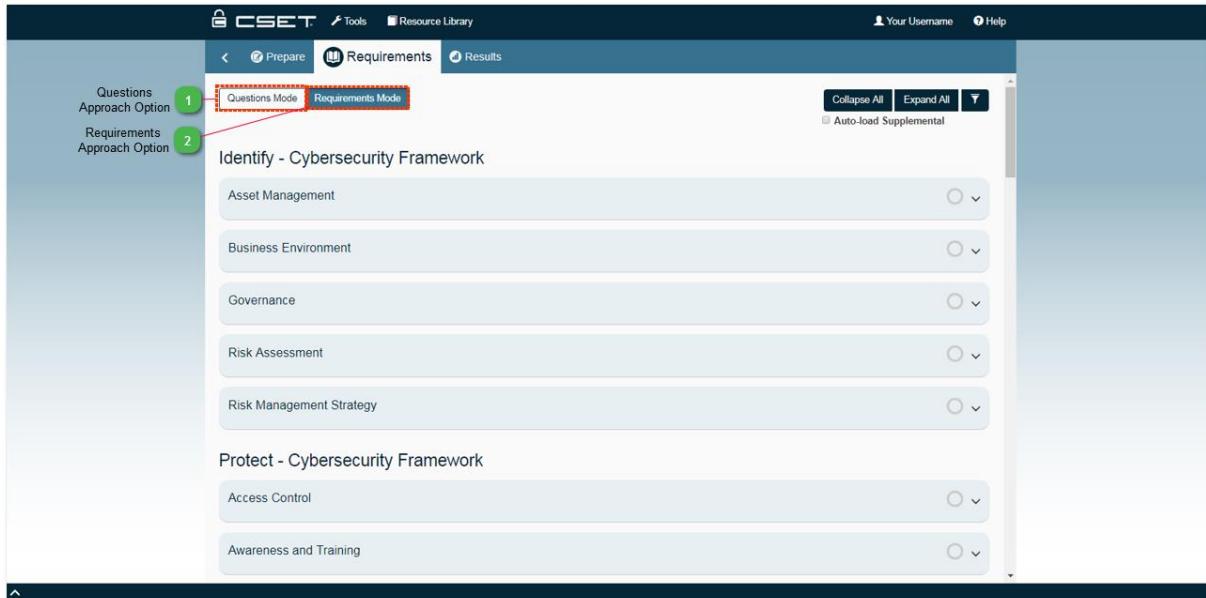


Figure: Mode Selection Screen

### 1 Questions Approach Option

Questions Mode

The Questions-based approach will ask simple questions during the assessment. The questions are determined from requirements based on the selected cybersecurity standard. All questions are scored in the final results. Most advanced users will select the Questions-based approach.

### 2 Requirements Approach Option

Requirements Mode

The Requirements-based approach uses the exact wording of requirements from the selected Standard as questions and each requirement must be fully met in order to meet the requirement. This approach is best used by industries that are regulated by a specific standard.

## Assessment Mode

This section provides additional information on the three available advanced assessment modes on the Assessment Mode Selection screen of the CSET tool.

### **Questions-based Approach:**

A comprehensive set of questions has been prepared with straightforward language that encompasses all the topics and requirements found in the major industrial control system (ICS) and information technology (IT) Standards. Each question is written in such a way that it can be answered as either Yes or No. (Questions can also be answered by using alternates or not applicable; however, they do not use multi-part answers.) The full set of questions is filtered and limited by the Standards selected and by the SAL. The Questions mode is recommended for most assessments and is set by default.

### **Requirements-Based Approach:**

The Requirements mode was developed primarily for regulated industries such as nuclear or electrical power. This mode is designed so that the user will see the exact wording of each requirement in the Standard. The question must be read and answered in its entirety.

### **Questions-based Approach**

If the Questions-based Approach is selected then most of the Standards will be available. Select the Standard or Standards that apply to the system and industry or sector being evaluated.

If only one Standard is selected, the Key Questions offer a small selection of the top set of requirements designed for assessments of limited scope or time while the Universal Questions offer the most comprehensive, general evaluation.

If multiple Standards are selected, the questions will be the superset of all selected Standards. It is recommended that the Universal Questions be included. The Standards may have some questions that are so unique that they are not included in the universal set. This means that selecting both the Universal Questions and a Standard will result in a set of questions that is potentially greater than the Universal Questions themselves. These situations are described in detail below.

In the Figure below, three cases are presented. (In 1 and 2, there is no consideration for the SAL.)



### Figure: Question Sets for Questions Mode

**Case 1.** In this scenario, only the Universal Questions option has been selected. As shown in the diagram, all the Universal Questions are displayed.

**Case 2.** This scenario shows two options. If only Standard A was selected, then only those questions included in the inner circle would be presented. The Universal Questions outside the inner circle would not be included in the assessment. The second option shows where both Standard A and the Universal Questions were selected. Because the Standard is completely included in the Universal Question set, the resulting assessment questions would look exactly like Case 1, the Universal Question set.

**Case 3.** Unlike the example in Case 2, the selected Standard B has extra questions not found in the Universal Question set. If only Standard B was selected then everything shown in the ellipse would be displayed in the assessment. If both the Standard and Universal Questions sets were selected, then the total assessment would be greater than what is included in Case 1 and would include the combination of both the round (Universal) and ellipse (Standard B) shapes.

## Requirements-based Approach

If the Requirements-based Approach is chosen, then the Universal Questions option is disabled. If multiple Standards are selected, then for each choice a completely different set of requirements will be displayed. In the Figure below, two cases are presented.

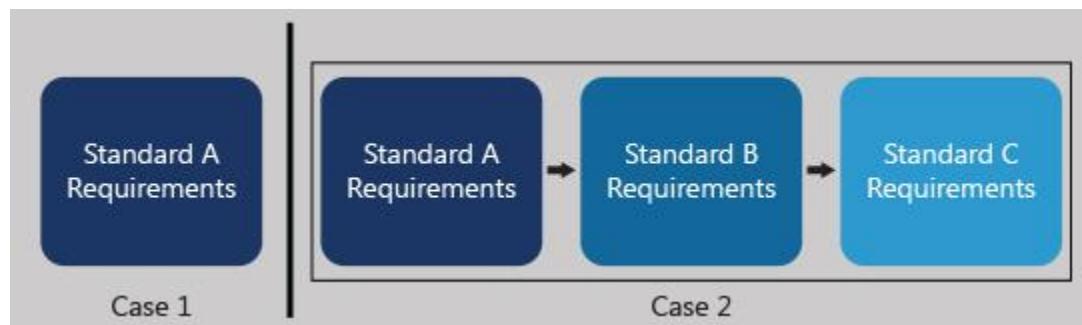


Figure: Requirements Mode

**Case 1.** In this scenario, a single Standard has been selected, and only the requirements for Standard A will be presented in the Questions screen.

**Case 2.** This second scenario shows the selection of multiple Standards. No matter how many Standards are selected, the tool will display the full set of requirements for each set regardless of any overlap. Because the wording in the Standard is unique, each requirement will be given verbatim. In the application, the requirements in the Standards will simply show up on the question tree in a sequential manner.

## Standards Available in Both Modes

Many Standards are available in both the Questions mode and the Requirements mode. In Questions mode, statements from the Standard may be split apart to form several questions so that the user may get partial credit for complying with a portion of the requirement. It also makes each question shorter, more direct, and easier to understand. In Requirements mode, the requirement statement is presented as written in the Standard. It may be longer and encompass several compliance activities. Partial compliance is considered a Fail in this mode.

## Assessment Section

The assessment section is where the user answers questions related to the selected Standards or Profile and Security Assurance Level. The following sections will describe the Assessment process in detail.

## Assessment Screen

The primary interaction that takes place in CSET happens on the Assessment screen. The Assessment screen displays sets of questions or requirements for the user to read and answer based on the selected assessment mode, the actual Standards chosen, the security assurance level (SAL), and the components used on the diagram tool. The results of the combined answers to the presented questions will help to provide a good perspective and understanding of the organization's cybersecurity posture.

Completing the questions portion of the assessment is where most of the time will be spent. The process of answering questions is not difficult but it can be tedious. It is recommended that the user plan ahead and recognize that it will take several hours or even days to accurately answer all the questions. The more time spent understanding the intent of each question and then discussing it as a team, the more valuable will be the assessment. Take the time to fully understand the intent of each question then provide the answer that best meets the current situation. If upgrades are in progress at the time of the assessment, comments can be associated with the relevant questions to document the activity.

The Assessment screen will display different content based on the selected assessment mode. For more information about the different content displayed based on the assessment mode, see the [Assessment Modes](#) help section.

The Figure below shows the main sections of the Assessment screen.

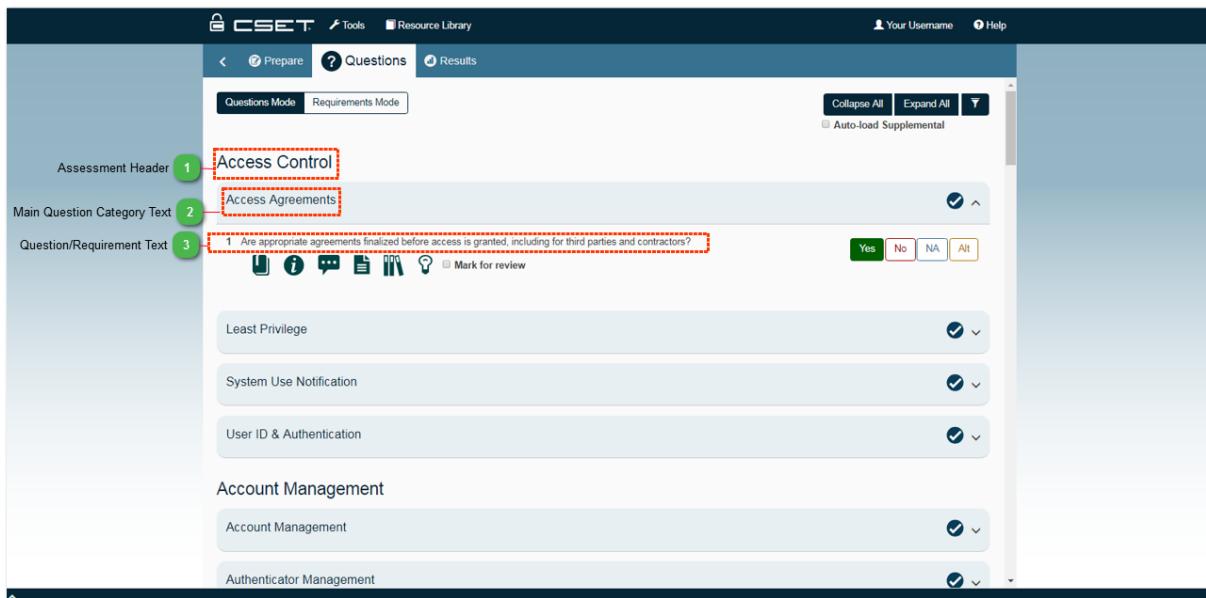


Figure: Assessment Screen

1

## Assessment Header

Access Control

The assessment header contains controls for managing the questions displayed in the Question/Requirement Text section.

2

## Main Question Category Text

Access Agreements

The green Main Question Category Text displays the high-level categories in which groups of questions or requirements belong.

3

## Question/Requirement Text

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

The Question/Requirement Text contains the questions and requirements of the assessment as well as the answers and supplemental information.

The answers for all questions will be Yes, No, Not Applicable, and Alternative Response. The process is simple. Read the question in detail and then answer yes if the question language and intent are met, or no if the question language and intent are not met. The colors of the answers reflect the answer given. The colors provide a quick visual reference of how the user is doing in each category.

Yes answers are green, No answers are red, Not Applicable answers are blue, and ALT answers are light green.

In addition to clicking the answers with the mouse, shortcut keys are available to use with this screen. The full list of keyboard shortcuts is available in the help section titled [Keyboard Shortcuts](#).

The Not Applicable is used when the question does not apply to the system or facility. It should be used with discretion and has the effect of removing the question from consideration. Any questions marked as Not Applicable will not show up in the online analysis or reports as a gap or missed answer; nor will they count as a positive answer.

The ALT label stands for Alternate and is used when an alternate or different method is being used to address the concern in the question. For example, a question may be asked about whether the servers are located behind locked doors with certain access restrictions. The facility may not have locked doors, but instead, employ a security guard at the door to the server room. This different (security guard) approach does not directly answer the question, but the user may feel like this alternate approach to securing the room is either equal to or better than locks on the doors. An alternate method is scored in a positive way similar to a Yes answer.

If an alternate method is selected, then the user should fill in the description in the Question Details panel in the text box under the label Alternate Description/Justification. The Question Details panel is opened when the Details tab is clicked.

## Assessment Modes

The questions on the assessment screen will change based on the assessment mode selected. Questions are organized into categories and different information is displayed based on the selected mode. There are three modes of operation that affect the display of questions:

1. Questions Mode,
2. Requirements Mode

### **Questions Mode**

The Assessment Screen in Questions mode displays simple to read questions on the Assessment screen. Next to the questions is Supplemental Information from the associated requirement in the related Standard.

The unique characteristics of the Assessment Screen in Questions mode are shown on the [Assessment Screen Questions Mode](#) page.

### **Requirements Mode**

The Assessment Screen in Requirements mode displays the exact wording of the requirement text in the associated Standard.

The unique characteristics of the Assessment Screen in Requirements mode are shown on the [Assessment Screen Requirements Mode](#) page.

## Assessment Screen Questions Mode

The Figure below displays the Assessment screen in Questions mode. Questions mode is the recommended assessment mode for most users.

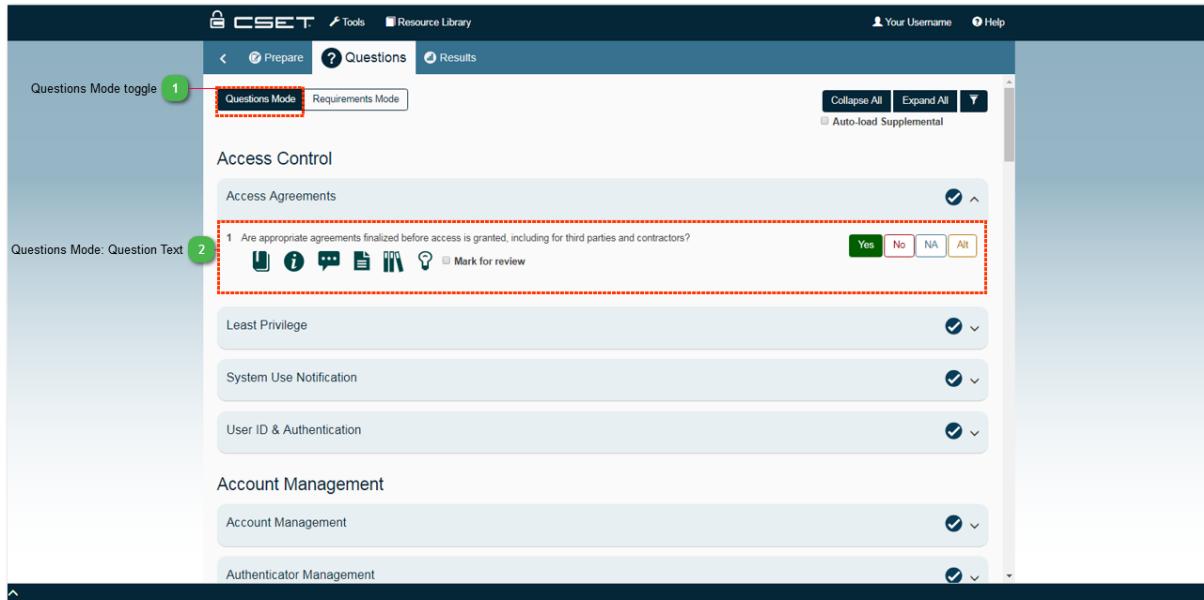


Figure: Assessments Screen in Questions Mode

1

### Questions Mode toggle

Questions Mode

The Questions Mode button is blue when selected. This indicates that the user is in the Questions Mode screen.

2

### Questions Mode: Question Text

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



Yes No NA Alt

Questions Mode questions have been prepared using straightforward language. The questions encompass all the topics and requirements found in the major ICS and IT Standards. The questions are generally fairly short compared to their associated requirements from the underlying Standard. The question text is typically a subset of the underlying requirement text.

# Assessment Screen Requirements Mode

The Figure below displays the Assessment screen in Requirements mode. Requirements mode is recommended for regulated industries where the exact wording of the Standard is important.

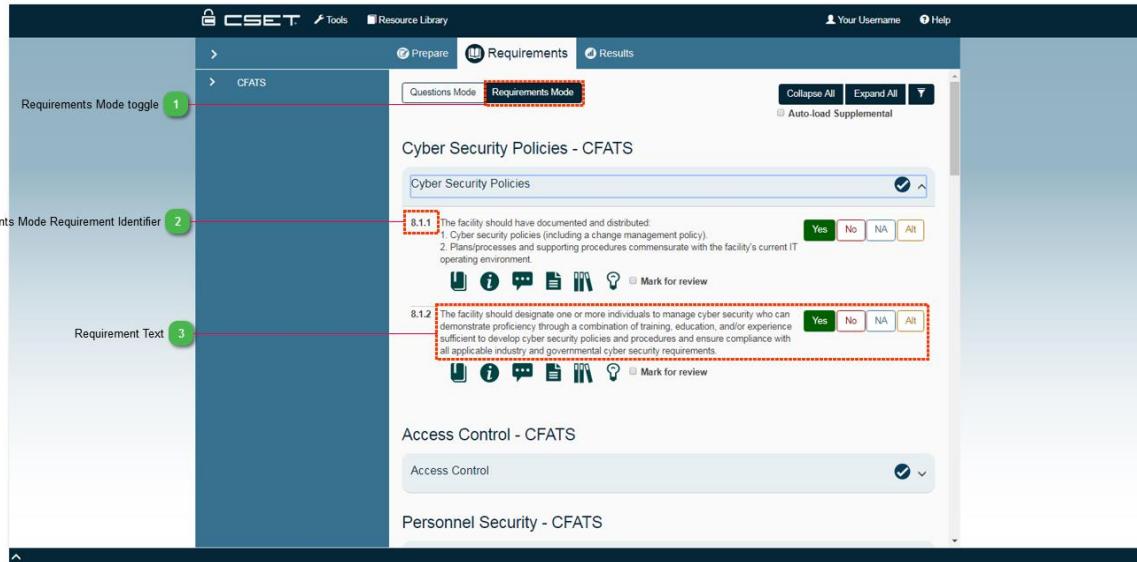


Figure: Assessment Screen in Requirements Mode

1

## Requirements Mode toggle

**Requirements Mode**

The Requirements Mode button is blue when selected. This indicates that the user is in the Requirements Mode screen.

2

## Requirements Mode Requirement Identifier

**8.1.1**

Requirements mode displays the Requirement Identifier instead of a question number.

3

## Requirement Text

The facility should designate one or more individuals to manage cyber security who can demonstrate proficiency through a combination of training, education, and/or experience sufficient to develop cyber security policies and procedures and ensure compliance with all applicable industry and governmental cyber security requirements.

**Yes**   **No**   **NA**   **Alt**

Requirement Text displays requirements directly from the standard for users to answer.

# Assessment Categories

Question sets are divided into categories depending on the assessment mode, Standards, and SAL selected. Different categories are displayed in multiple areas on the Questions screen based on the Assessment mode such as the bread crumb navigation control, the titles above the questions, and In the Question Details Section.

The Figure below shows some examples of Question Categories in Questions mode. Requirements mode doesn't display the Sub Category Text.

The screenshot shows the CSET software interface in 'Questions Mode'. At the top, there are tabs for 'Prepare', 'Questions' (which is selected), and 'Results'. Below the tabs, there are buttons for 'Questions Mode' and 'Requirements Mode', and controls for 'Collapse All', 'Expand All', and 'Auto-load Supplemental'. The main area displays a question card. The 'Main Category Text' is 'Access Control' (labeled 1). The 'Sub Category Text' is 'Access Agreements' (labeled 2). The 'Standard Specific Text' contains the requirement: 'The facility should ensure that service providers and other third parties with responsibilities for cyber systems have appropriate personnel security procedures/practices in place commensurate with the personnel security requirements for facility employees.' (labeled 3). Below the question card, there are three more items: 'Least Privilege', 'System Use Notification', and 'User ID & Authentication', each with a checked checkbox.

Figure: Question Categories

1

## Main Category Text

Access Control

All questions in CSET have been grouped into main categories. The main categories are high level groupings for questions and are used as high level groupings for improved navigation and in the assessment results.

2

## Sub Category Text

Access Agreements

Sub categories are lower level categories in which questions are grouped. The sub categories contain fewer questions than the universal categories.

3

## Standard Specific Text

### Standard Specific Requirement:

The facility should ensure that service providers and other third parties with responsibilities for cyber systems have appropriate personnel security procedures/practices in place commensurate with the personnel surety requirements for facility employees.

The Standard Specific text is the category associated with the question in the requirement text of the associated Standard. The Standard Requirement Category can be found in associated reference documentation related to each question.

# Question Details, Resources, and Comments

The Question Details, Resources, and Comments contains extra detailed information about the currently selected question. The user can also add comments, discoveries, and reference documents to the question or requirement as well as mark the question or requirement for further review. The Figure below describes the Question Details, Resources and Comments screen.

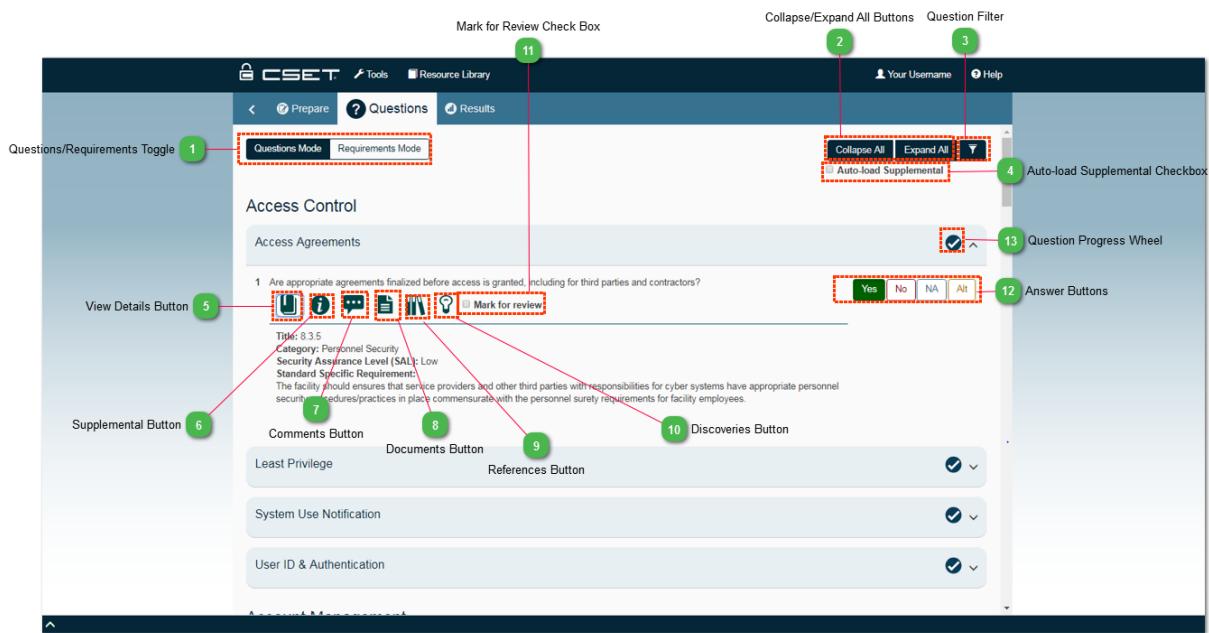


Figure: Question Details, Resources, and Comments Screen

**1**

## Questions/Requirements Toggle



The Question/Requirements toggle allows a user to switch between Question and Requirements mode.

**2**

## Collapse/Expand All Buttons



Click the Collapse All button to close all question categories, and the Expand All button to open all question categories.

**3**

## Question Filter



Clicking the Question Filter allows the user to filter the assessment questions by answer, whether an assessment has comments, discoveries, or has been marked for review.

4

## Auto-load Supplemental Checkbox



Clicking the Auto-load Supplemental checkbox will automatically load supplemental information as the user scrolls through questions.

5

## View Details Button



The View Details button will show or hide the details for each question.

See the [Details Section](#) for more information.

6

## Supplemental Button



Clicking the Supplemental button opens up the supplemental information for the questions.

See the [Supplemental Section](#) for more information.

7

## Comments Button



Clicking the Comments button opens the Comments Section of the Details and Resources panel allowing the user to enter comments related to the current question or requirement.

See the [Comments Section](#) for more information.

8

## Documents Button



Clicking the Documents button opens the Documents section of the Details and Resources panel allowing the user to associate related documents to the question or requirement.

See the [Documents Section](#) for more information.

9

## References Button



Clicking the References button opens the References section of the Details and Resources panel allowing the user to open Standards that are associated with and referenced in the assessment question.

See the [References Section](#) for more information.

10

## Discoveries Button



Clicking the Discoveries button opens the Discoveries section of the Details and Resources panel allowing the user to create a discovery record to associate to the question or requirement.

See the [Discoveries Section](#) for more information.

11

## Mark for Review Check Box



The Mark for Review Check Box allows the user to mark a question or requirement for future review.

12

## Answer Buttons



Click "Yes", "No", "NA", or "Alt" to answer questions.

13

## Question Progress Wheel



The Question Progress Wheel indicates how many questions a user has filled out. The checkmark means that all questions in the category have been answered.

## Details Section Question Mode

The Question or Requirements Details section will contain different controls and text depending on the selected assessment mode. The Figure below describes the Details section in Question Mode.

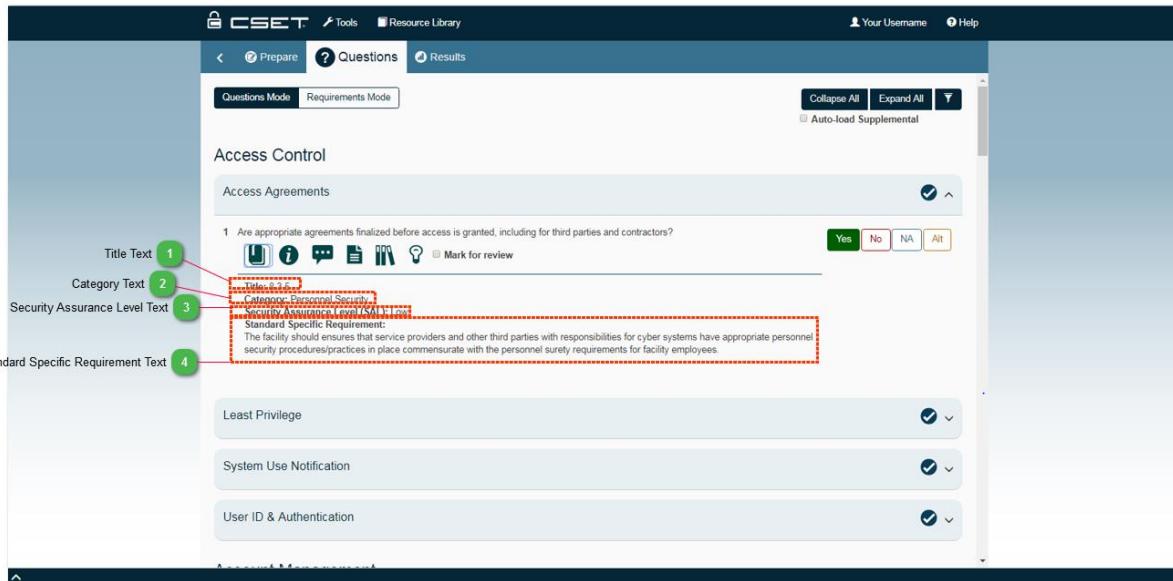


Figure: Details Section Question Mode Panel

1

### Title Text

**Title: 8.3.5**

The Title text is a textual identifier for the question usually related to the Standard to which it belongs.

2

### Category Text

**Category: Personnel Security**

The Category text is the Standard category of the question. Questions typically reside in multiple categories. The Category text here indicates the category in the related Standard to which that the question belongs.

For more information about question categories, see the [Assessment Categories](#) help section.

3

### Security Assurance Level Text

**Security Assurance Level (SAL): Low**

The Security Assurance Level text is the highest SAL of the question. All questions and requirements have SAL value assigned to them. The Security Assurance Level text

indicates the SAL for the question. When users select a SAL and a Standard during the preparation process, they will get all questions in their selected Standard that have the same or lower SAL they selected. For example, if users selected a High SAL and the Key Standard, they will get all questions in Key that are High, Medium, and Low.

4

## Standard Specific Requirement Text

### Standard Specific Requirement:

The facility should ensure that service providers and other third parties with responsibilities for cyber systems have appropriate personnel security procedures/practices in place commensurate with the personnel security requirements for facility employees.

The Standard Specific Requirement text is the requirement text from the Standard associated with the question. If the user is in the Requirements assessment mode, the Standard Specific Requirement text will be the same as the question text. Note: There are also many instances where Standard Specific Requirement text will be the same as the question text.

## Details Section Requirements Mode

The Question or Requirements Details section will contain different controls and text depending on the selected assessment mode. The Figure below describes the Details section in Requirements Mode.

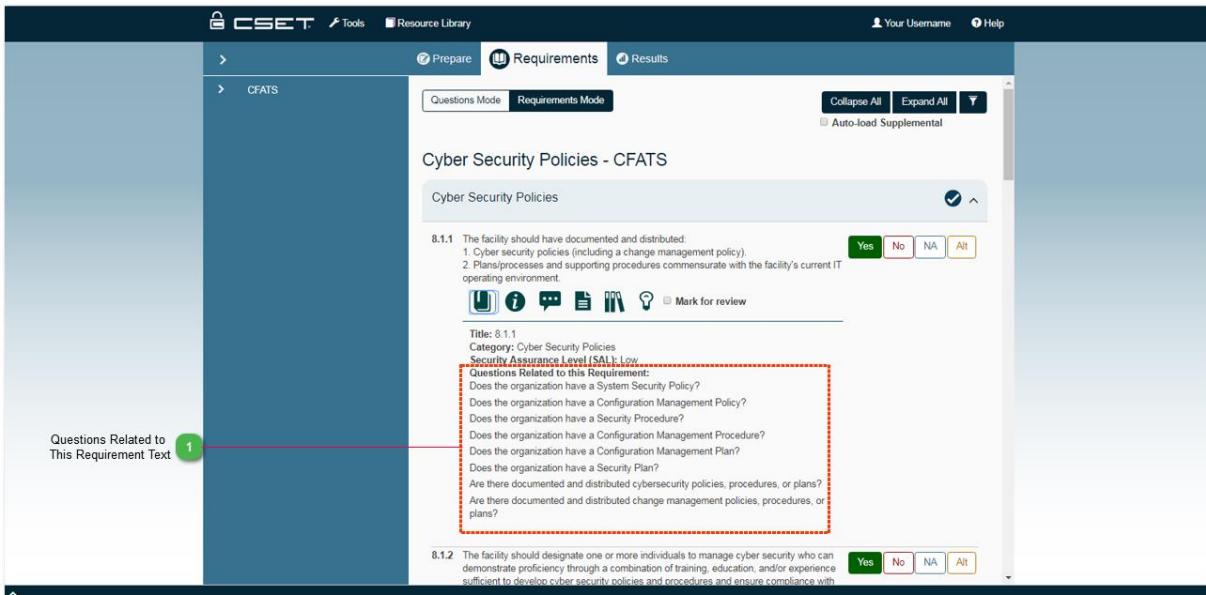


Figure: Details Section Requirement Mode

### 1 Questions Related to This Requirement Text

#### Questions Related to this Requirement:

- Does the organization have a System Security Policy?
- Does the organization have a Configuration Management Policy?
- Does the organization have a Security Procedure?
- Does the organization have a Configuration Management Procedure?
- Does the organization have a Configuration Management Plan?
- Does the organization have a Security Plan?
- Are there documented and distributed cybersecurity policies, procedures, or plans?
- Are there documented and distributed change management policies, procedures, or plans?

The main difference between the Question and Requirements modes is that Requirements Mode has the extra Questions Related to this Requirement text. The Questions Related to this Requirement text displays all questions identified by the Requirement.

## Supplemental Section

Questions and Requirements on the Assessment screen will almost always have supplemental information. The Figure below describes the assessment screen focusing on Supplemental information.

The screenshot shows the CSET software interface. At the top, there's a navigation bar with 'CSET', 'Tools', 'Resource Library', 'Your Username', and 'Help'. Below that is a toolbar with 'Prepare', 'Questions' (which is selected), and 'Results'. Underneath are 'Questions Mode' and 'Requirements Mode' buttons, and 'Collapse All', 'Expand All', and 'Auto-load Supplemental' buttons. The main content area is titled 'Access Control' under 'Access Agreements'. It contains a question: '1 Are appropriate agreements finalized before access is granted, including for third parties and contractors?'. To the right of the question are four buttons: 'Yes' (green), 'No' (red), 'NA' (blue), and 'Alt' (orange). Below the question is a red-bordered box containing the supplemental text: 'Managing relationships with external service providers, business partners, and vendors should be considered so that they do not compromise the security of an organization.' A green circle with the number '1' is overlaid on the left side of this supplemental text box.

Figure: Question Supplemental Information

### 1 Question Supplemental Information Text

Managing relationships with external service providers, business partners, and vendors should be considered so that they do not compromise the security of an organization.

The supplemental text is a readable explanation and elaboration of the subject found in the question or requirement. The text is typically taken from the Standard itself. So questions may exist that do not have supplemental information if they were not included in the Standard. If a set of questions was taken from a single long requirement, the supplemental text may be repeated for multiple questions.

## Comments Section

CSET allows the user to add comments to any assessment question or requirement during the assessment process. The Figure below describes the comment process.

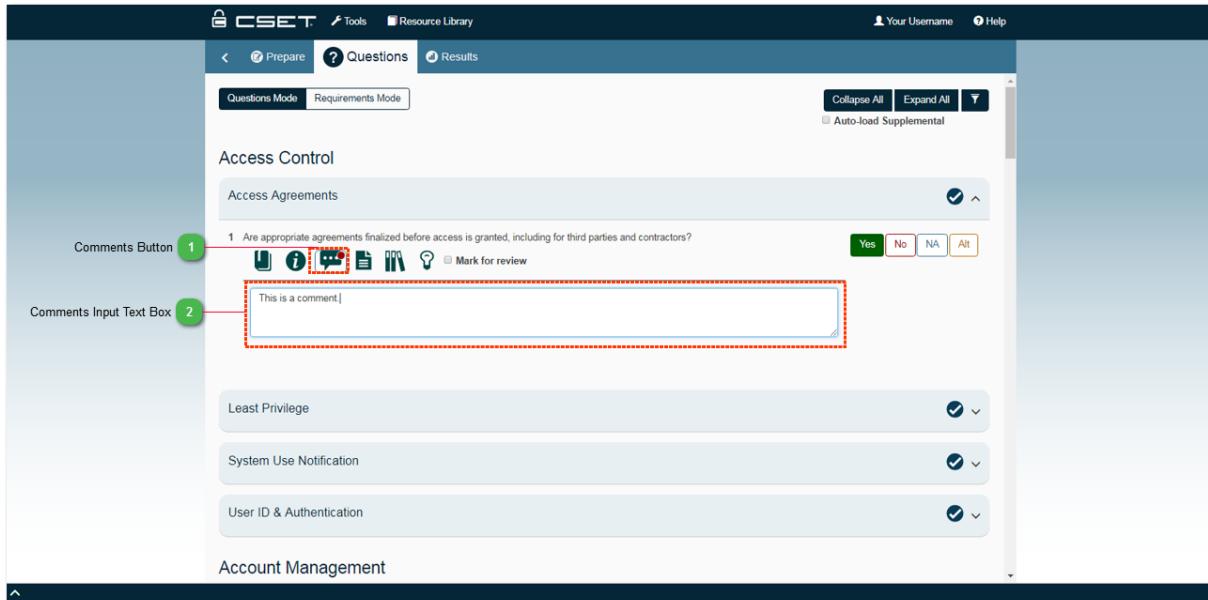


Figure: Assessment Screen Comments Section

1

### Comments Button



The Comments button displays a red dot over the comments icon when the question or requirement has comments. This allows the user to easily see what questions have comments when scrolling through the list of questions.

2

### Comments Input Text Box

This is a comment.

A screenshot of a text input field containing the text 'This is a comment.' The field has a light blue border and a cursor at the end of the text.

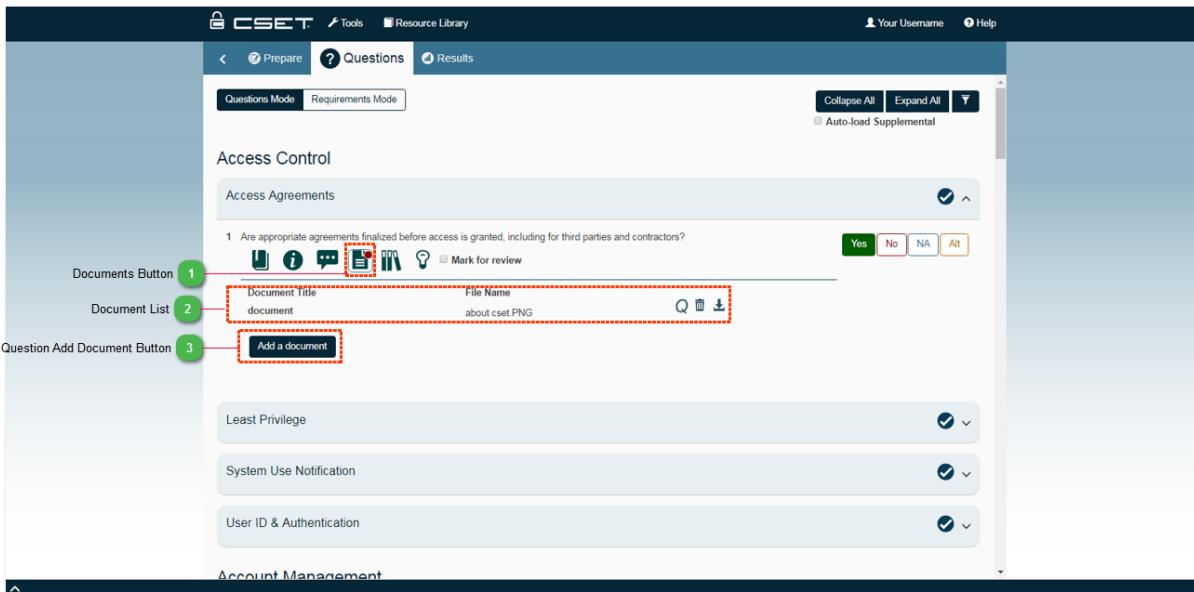
The Comments text box allows the user to add comments or other textual information related to a question or requirement. Comments can be added for multiple reasons such as implementation details, reasons for marking a question for review, answer justifications, etc.

In some assessments, the Comments input text box is used on rare occasions; in others, the comments are used to record the verification method of answers. This field can be a powerful tool to support the quality of the assessment, especially when

documents are also attached to support the answer using empirical data.

## Documents Section

CSET allows the user to associate documents to any assessment question or requirement during the assessment process. The Figure below describes the document process.



**Figure: Documents Section**

1

### Documents Button



The Question Documents button displays a red dot over the Document icon when the question or requirement has associated documents. This allows the user to easily see what questions have associated documents when scrolling through the list of questions.

2

### Document List

Document Title	File Name	
document	about cset.PNG	

The Question Document List displays all documents currently associated with the selected question. It displays the document title and file name as well as the Associated Questions button, Remove Document button, and Export Document button. The File Name is the name of the physical file with its file extension.



### Remove Document button

The Remove Document button allows the user to remove the association between a document and a question. If the document isn't associated with another question, it will

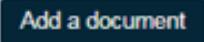
remove the document from the assessment.

### Download Document button

The Download Document button allows the user to download a document from the assessment so it can be reviewed. Clicking the Download Document button will save a copy of the document file to a specified location.

3

## Question Add Document Button

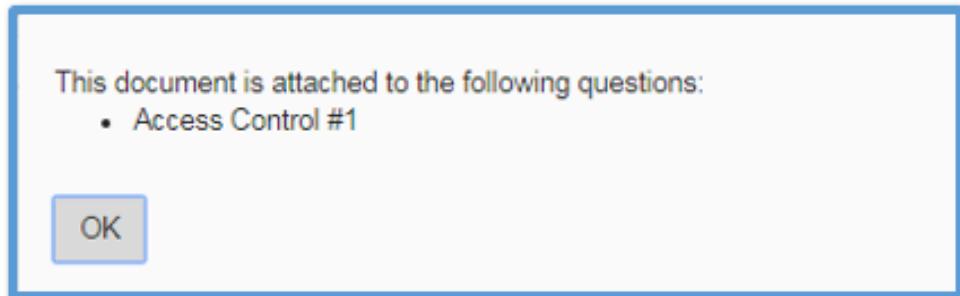


Add a document

Clicking the Add Document button will open an "Open File" dialog window allowing the user to navigate to a document file to associate with the question or requirement. Once selected, the document will be displayed in the Question Document List below the Add Document button.

## Questions List

The Question List window shows the name of the referenced document and a list of all questions associated with that document as seen in the Figure below.



**Figure: Questions List Window**

## References Section

The References Section contains links to related source and Help documentation as seen in the Figure below.

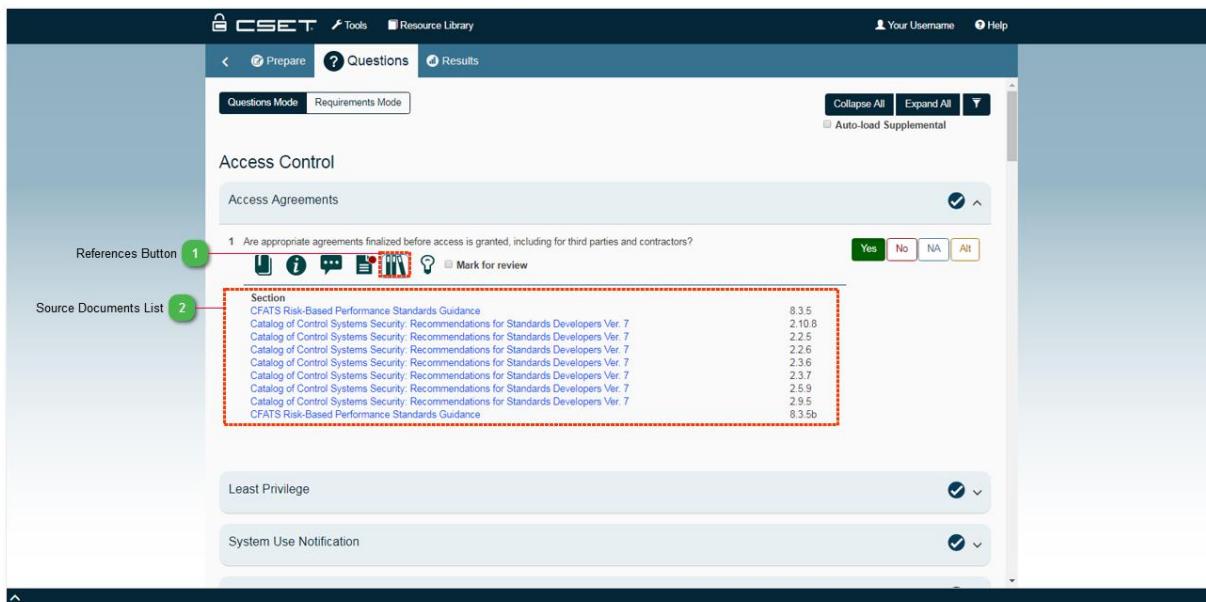


Figure: Question Details References Section

1

### References Button



The References button displays all references related to the question/requirement.

2

### Source Documents List

Section	
CFATS Risk-Based Performance Standards Guidance	8.3.5
Catalog of Control Systems Security: Recommendations for Standards Developers Ver. 7	2.10.8
Catalog of Control Systems Security: Recommendations for Standards Developers Ver. 7	2.2.5
Catalog of Control Systems Security: Recommendations for Standards Developers Ver. 7	2.2.6
Catalog of Control Systems Security: Recommendations for Standards Developers Ver. 7	2.3.6
Catalog of Control Systems Security: Recommendations for Standards Developers Ver. 7	2.3.7
Catalog of Control Systems Security: Recommendations for Standards Developers Ver. 7	2.5.9
Catalog of Control Systems Security: Recommendations for Standards Developers Ver. 7	2.9.5
CFATS Risk-Based Performance Standards Guidance	8.3.5b

There will always be at least one source document for the selected Standard. If there is more than one source, then all the sources will be shown in the list of hyperlinks under the title. If the Universal set was selected, then the source will typically be the DHS Catalog of Control Systems Security: Recommendation for Standards Developers, Version 7, often referred to as the Catalog of Recommendations or CoR. If another Standard was selected, then that Standard document would be the source. In most cases, the document will open to the section where the requirement is found.

## Discoveries Section

The Discoveries Section of the question details allows the user to associate Discovery information with a question or requirement. The Figure below shows the Question Details Discovery Section.

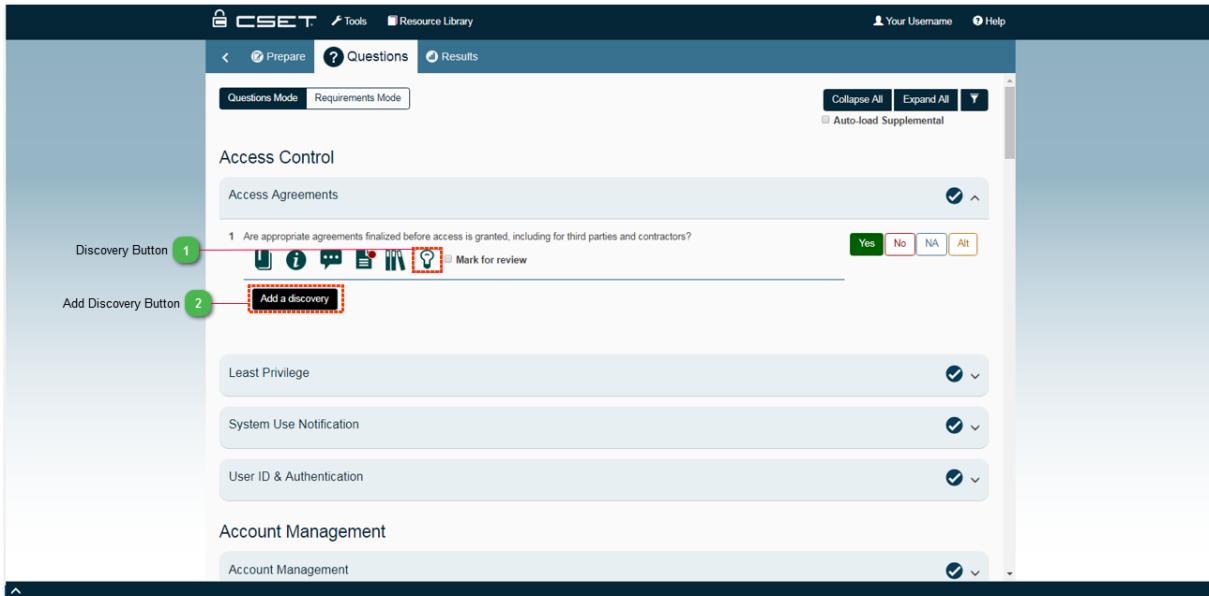


Figure: Details Discoveries Section

1

### Discovery Button



The Discovery button displays a red dot over the Discovery icon when the question or requirement has associated discoveries. This allows the user to easily see what questions have discoveries when scrolling through the list of questions.

2

### Add Discovery Button

**Add a discovery**

Clicking the Add Discovery button opens the Discoveries Window that allows the user to enter all question discovery related information.

For more information about the Discoveries Window, see the [Question Discoveries](#) help section.

## Question Discoveries

The Question Discoveries window allows the user to enter information about a question or requirement that has a no answer. Any question or requirement that has been answered "No" could potentially have a discovery record. The discovery records provide information about the issue, potential impacts of the issue, recommendations for rectifying the issue and potential vulnerabilities related to the issue. Responsible individuals can also be assigned to discovery records to be responsible for fixing the problems associated with the discovery record. The Figure below describes the different parts of the Question Discoveries window.

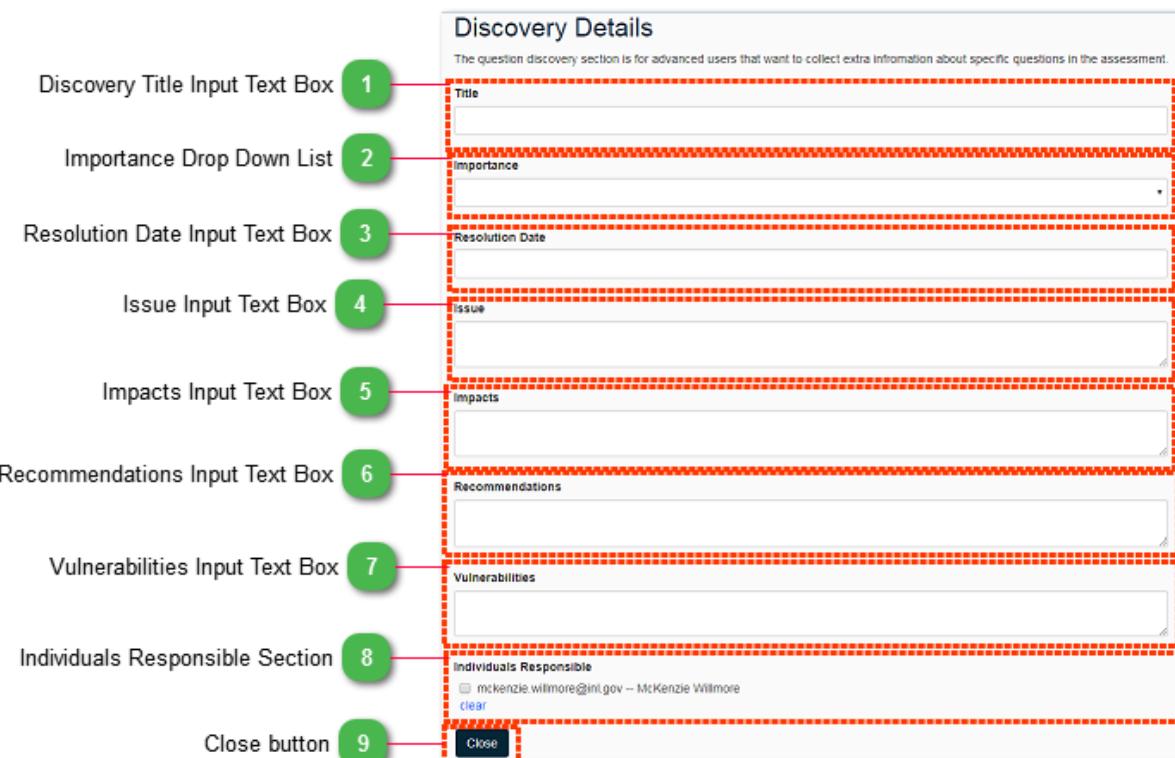


Figure: Discovery Details Window

1

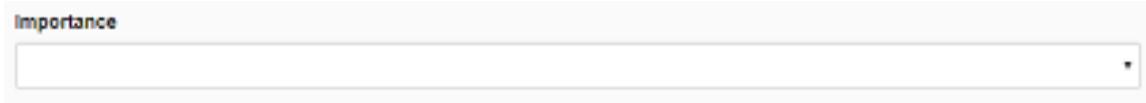
### Discovery Title Input Text Box

A screenshot of the 'Discovery Title Input Text Box' section. It shows a label 'Title' above a text input field containing a placeholder 'Title'.

The Discovery Title input text box corresponds to a Title or Name for the Discovery record to help the user identify it.

2

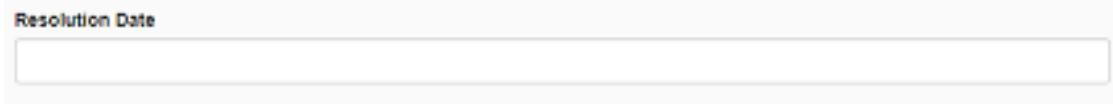
### Importance Drop Down List



The Importance drop down list allows the user to assign an importance level to the discovery record. Valid values are Low, Medium, and High.

3

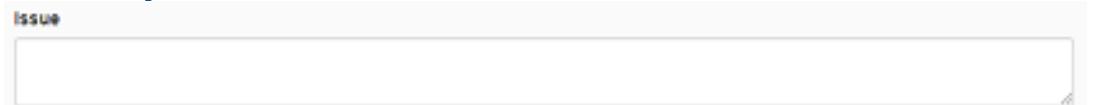
## Resolution Date Input Text Box



The Resolution Date input text box provides input for entering a date when the issue should be resolved.

4

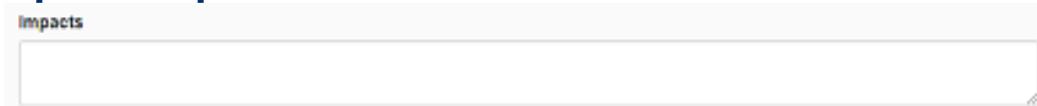
## Issue Input Text Box



The Issue input text box allows the user to define a detailed explanation of the issue or problem related to why the question or requirement was answered "No".

5

## Impacts Input Text Box



The Impacts input text box allows the user to define potential or real impacts that the issue may or is currently having on systems, assets, and/or procedures.

6

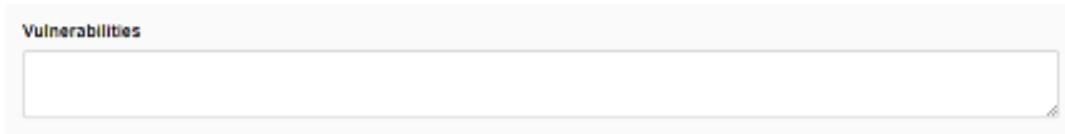
## Recommendations Input Text Box



The Recommendations input text box allows the user to provide recommendations or steps for resolving the issues or problems defined in the discovery.

7

## Vulnerabilities Input Text Box



The Vulnerabilities input text box allows the user to identify any known vulnerabilities on systems or assets related to the discovery.

8

## Individuals Responsible Section

A screenshot of a software interface titled "Individuals Responsible". It shows a list with one item: "mckenzie.willmore@int.gov -- McKenzie Willmore" followed by a "clear" link.

The Individuals Responsible section allows the user to assign individuals to be responsible for fixing the issues identified in the discovery record. The Contacts check list will contain a list of all current contacts associated with the assessment. Selecting a contact will associate an individual to be responsible for the Discovery record.

9

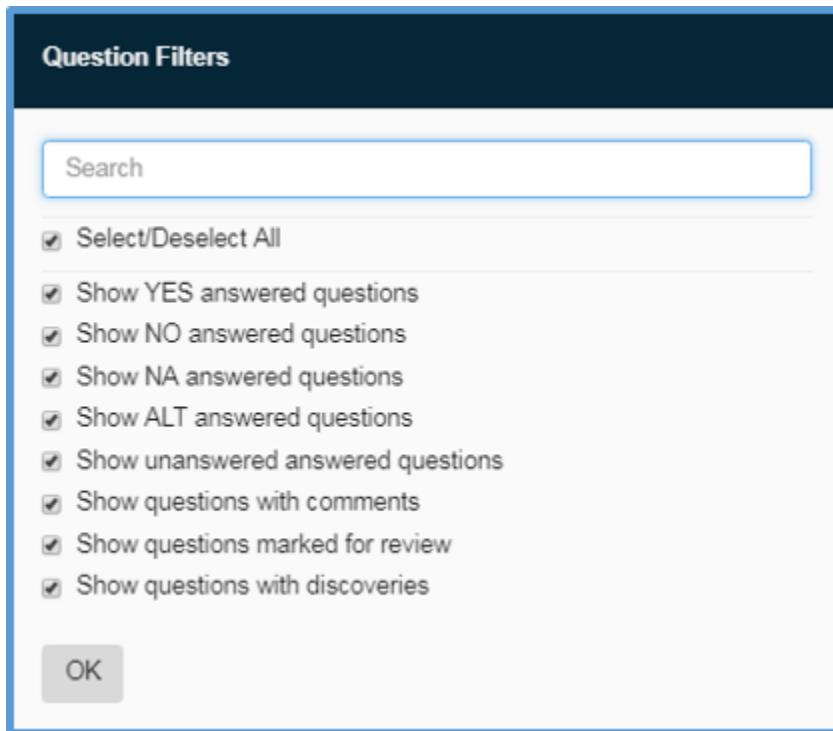
## Close button



The Close button will close the Question Discoveries window.

## Question Filter

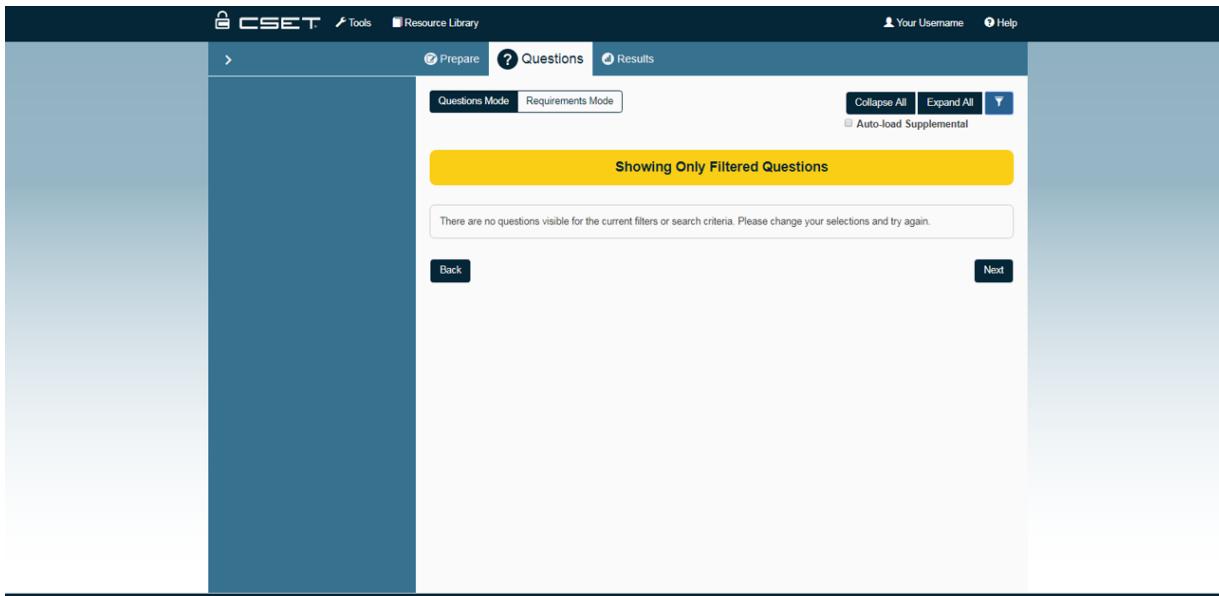
Use the Question Filter to limit the Question types you see. The user can filter on answer type (Yes, No, NA, Alt, Unanswered) or added discoveries, comments, and marked for review.



**Figure: Question Filter**

The user can select as many filters as they would like to combine, select all, or select none.

A message will appear if there are no results to show, so that the user can change their selection.



**Figure: No results visible error message**

## Results Section

Once Standards and SAL have been selected and the resulting questions have been answered, it is time to analyze the results of the assessment. Two methods are available to review and analyze the results. The first uses the online Results screens and the second approach is to print the reports and review the hardcopy.

The Results section provides a method to measure security posture based on the selected Standards and the questions answered during the assessment process. The Results section uses charts and tabular data to provide a visual display of the data and at the same time allows for comparisons across categories, questions, and subject areas.

The Results sections consists of the Analysis Dashboard and charts, and the Reports. This section will describe each area.

## Analysis Screen

The Analysis screen provides a quick visual view of how well the user is doing related to the user's cybersecurity posture. The Analysis screen consists of the Analysis Navigation Section, the Chart Section, and Results Navigation Section.

The Figure below describes the sections of the Analysis screen.

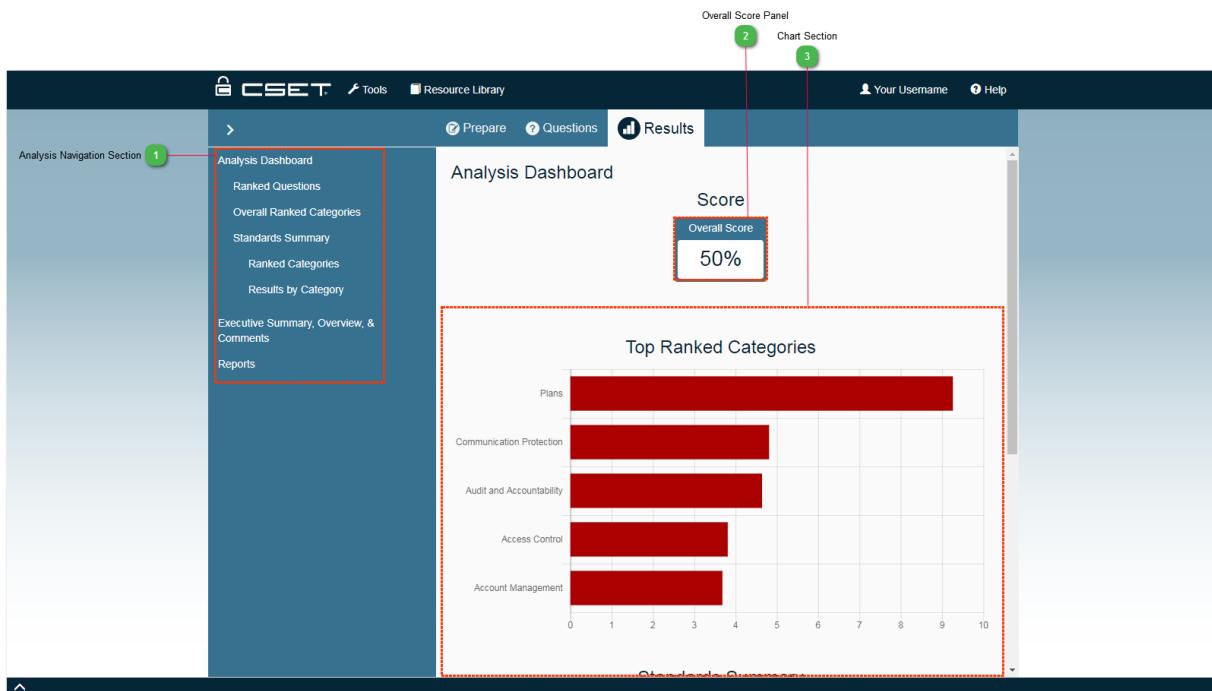


Figure: Analysis Screen

1

## Analysis Navigation Section



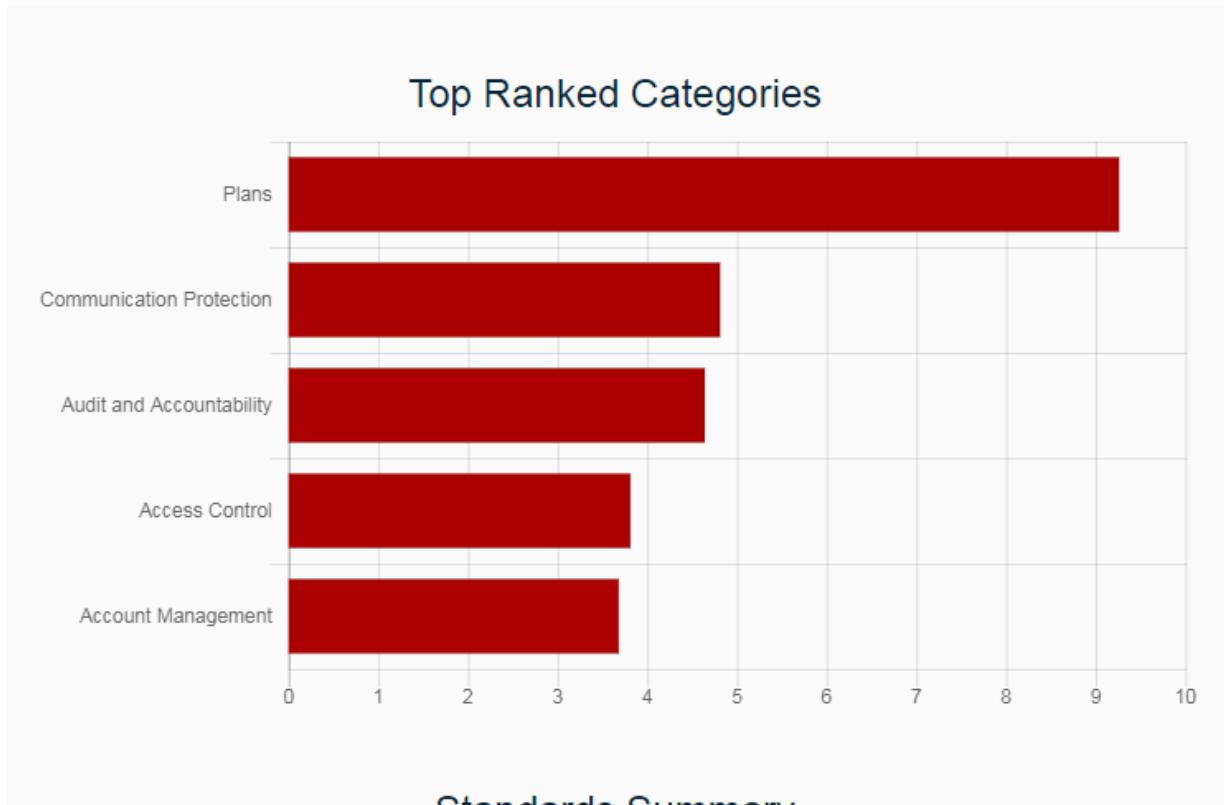
2

## Overall Score Panel



3

## Chart Section



The Chart section is where the charts and tabular data are displayed. Generally, the user can place the mouse cursor over a chart section to see the value associated with the section of the chart. Tabular data are also available to view or export on most screens.

## Dashboard in Questions/Requirements Mode

The Analysis Dashboard in Questions or Requirements mode shows four charts for quick reference. The charts displayed in the Questions/Requirements assessment mode are Assessment Compliance, Top Ranked Categories, Standards Summary, and Components Summary. The Figure below provides a brief description of the Dashboard in the Questions/Requirements assessment mode.

### Top Ranked Categories:

The Top Ranked Categories chart provides a quick look at the top six categories where the user needs to improve the most or the highest priority categories on which to focus attention first based on the assessment answers.

For more information about the Top Ranked Categories chart and data, see the [Overall Ranked Categories](#) help section.

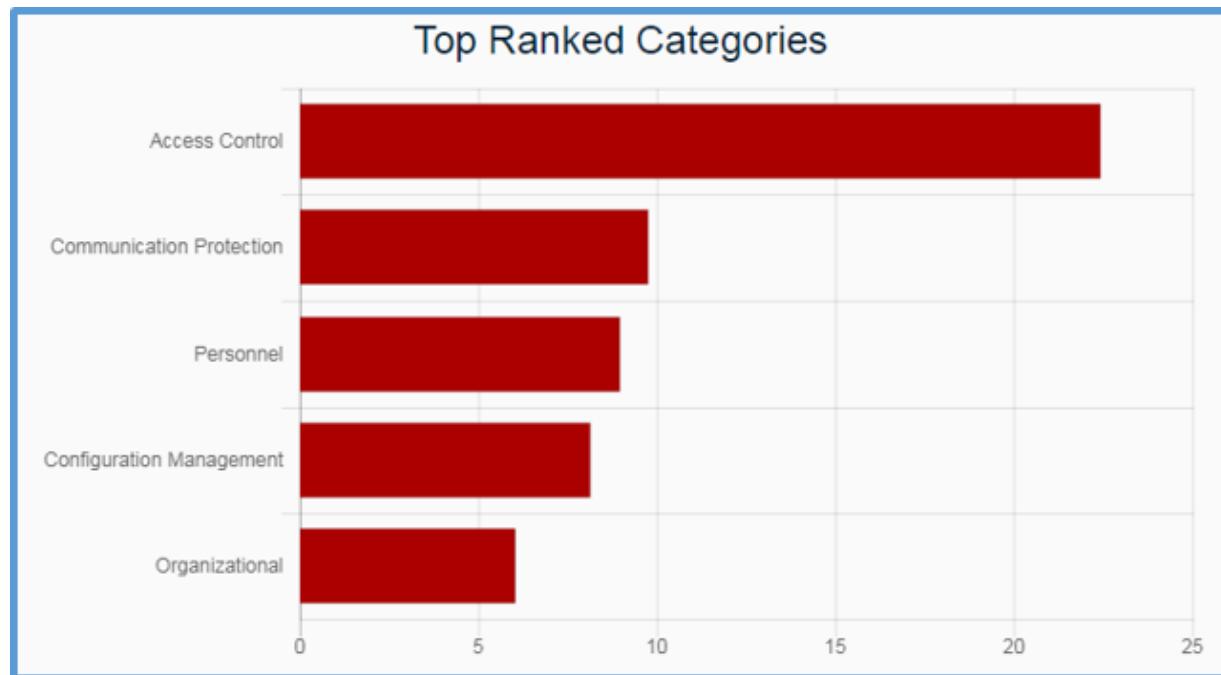


Figure: Top Ranked Categories Chart

### Standards Summary:

The Standards Summary chart provides a quick look at the percentages of how the user answered the Standards-based questions.

For more information about the Standards Summary chart and data, see the [Standards Summary](#) help section.

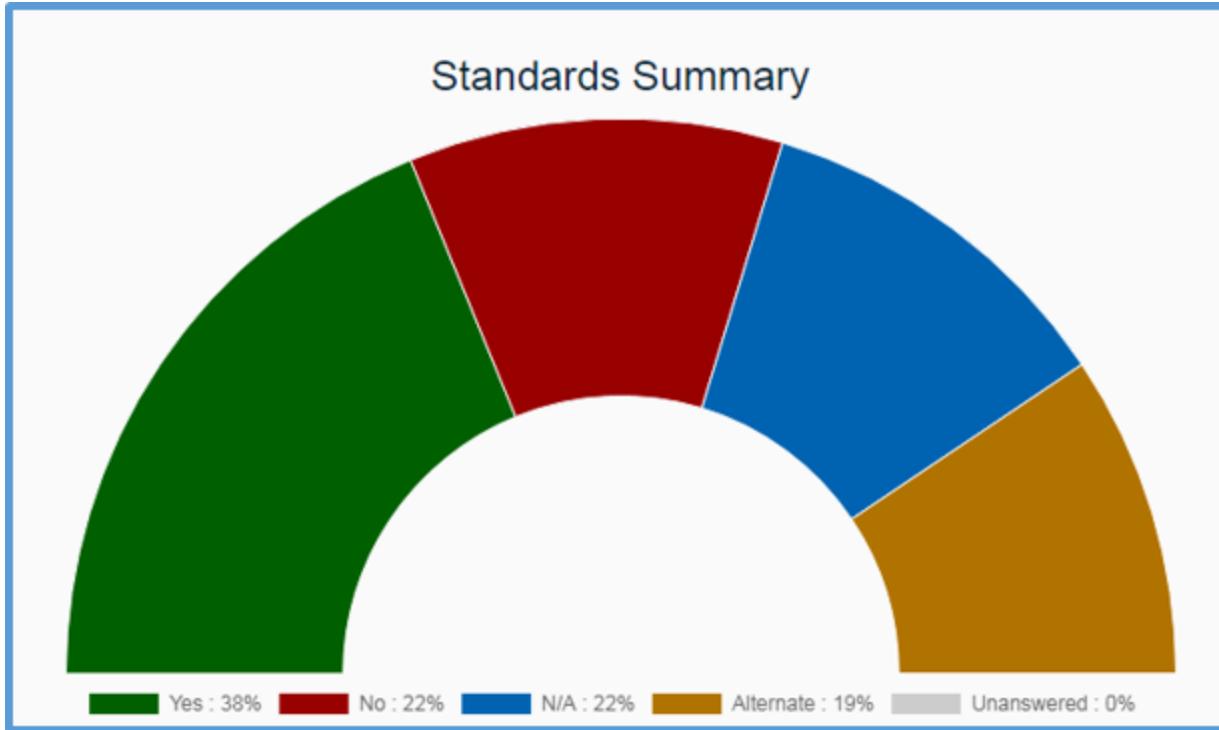


Figure: Standards Summary Chart

## Ranked Questions

Each question in the assessment where the answer had a No response or was unanswered will be ranked and displayed on the Ranked Questions Screen. The information provided is intended to answer the fundamental question, "Okay, I have some problems, so what do I do first?" Based on the ranking, the answer would be, do Number 1 first, and then do Number 2, and so on until all resources have been exhausted or all the problems have been resolved.

The Ranked Questions screen is shown in the Figure below.

The screenshot shows the 'Ranked Questions List' page. At the top, there's a navigation bar with tabs: 'Prepare', 'Requirements', and 'Results'. The 'Results' tab is active and highlighted with a green circle containing the number 2. On the far left, a sidebar has a 'Ranked Questions Navigation Button' (highlighted with a red box and number 1) which points to the 'Ranked Questions' link in the 'Analysis Dashboard' menu. The main content area is titled 'Ranked Questions' and contains a table with six rows of data. Each row includes a rank, standard, category, question text, and an 'Answer' column showing 'N' (No response).

Rank	Standard	Category	#	Question	Answer
1	CFATS	Access Control	6	Is the concept of least privilege used to accomplish assigned tasks?	N
2	CFATS	Plans	7	Does the security plan define and communicate the specific roles and responsibilities in relation to various types of incidents?	N
3	CFATS	Plans	13	Is the authorizing official or designated representative who reviews and approves the system security plan specified?	N
4	CFATS	Continuity	1	Does the alternate processing site provide information security measures equivalent to that of the primary site?	N
5	CFATS	Remote Access Control	1	Are the terms and conditions established for authorized individuals to access the system from an external system?	N
6	CFATS	Training	6	Is the knowledge of personnel on security policies and procedures based on their roles and responsibilities documented and	N

Figure: Ranked Questions Screen

### 1 Ranked Questions Navigation Button

Ranked Questions

Clicking the Ranked Questions button will show the Ranked Questions analysis screen.

### 2 Ranked Questions List

## Ranked Questions

Information on question ranking can be found in the [User Guide](#).

Rank	Standard	Category	#	Question	Answer
1	CFATS	Access Control	6	Is the concept of least privilege used to accomplish assigned tasks?	N
2	CFATS	Plans	7	Does the security plan define and communicate the specific roles and responsibilities in relation to various types of incidents?	N
3	CFATS	Plans	13	Is the authorizing official or designated representative who reviews and approves the system security plan specified?	N
4	CFATS	Continuity	1	Does the alternate processing site provide information security measures equivalent to that of the primary site?	N
5	CFATS	Remote Access Control	1	Are the terms and conditions established for authorized individuals to access the system from an external system?	N
6	CFATS	Training	6	Is the knowledge of personnel on security policies and procedures based on their roles and responsibilities documented and maintained?	N

The Ranked Questions list displays a list of all questions that were answered 'No' or left unanswered. The following is a description of the columns in the Ranked Question List:

### Rank:

A numeric ranking of each question that was missed with #1 having the highest priority.

The ranking is based on a combination of factors that all impact the overall score. The factors include the following:

#### **The specific weighting value assigned to each question in CSET.**

This weighting comes from subject matter experts with years of experience in information technology and control system cybersecurity. The questions were analyzed and assigned a weight relative to all other questions.

**The weighting value of the subject area or question category.** Each area was also given a weight by experts relative to all other areas. Like the question itself, it was determined that some areas are more important than others, even though they are all important to cybersecurity.

**The security assurance level (SAL) of the question.** Each question is

linked to an assurance level. For example, a question that is associated with a Very High level would be lower in rank than one with a Low level, because it is recommended that the user work on the basic requirements before moving to those required for a higher level. A good example relates to access control. Users should implement a complex password, (or maybe even a password) before worrying about implementing system access controlled by a combination of a complex password, physical token, and biometrics. The SAL will only affect the weighting when the score is higher than a Low for the facility. Because the SAL limits the questions to only those matching the SAL value, if the score is at a Low, then the user would never see any questions that might be marked as Moderate, High, or Very High.

**Standard Name:**

The value in this column identifies the Standard from which the question came. This concept is especially important when using multiple Standards that have the same category names. The combination of Standard Name, Category, and # will help locate the exact question or requirement.

**Category:**

The title of the main question category or subject area where the question or requirement is found.

**Number or #:**

This column identifies the question number in the Standard and category. The content is a hyperlink that when clicked, will open the Question screen and navigate to that question. The number will be the requirement title when in the requirements assessment mode.

**Question:**

The text from the question or the requirement, depending on which mode was selected.

**Answer:**

This is the answer selected when completing the assessment.

The data can be sorted by clicking its corresponding column header but it is recommended to keep the questions in Ranked order and address them accordingly.

## Overall Ranked Categories

The Overall Ranked Categories screen shows a list of all main categories ranked in order of the categories that should be prioritized based on how the questions were answered. Both Standards answers and diagram component answers are included on the chart and data. The chart shows the categories ranked in order of importance.

These categories are ordered by rank and indicate categories that need the most attention. Unlike other analysis screens that highlight the positive answers, this screen and the associated data show what categories or areas are weakest and what needs the most attention. In other words, the longer the bar in the chart, the worse it scored in that area.

The Data tab contains the tabular data of the categories that match the bars on the associated chart. There are five columns in the tabular data:

### **Category:**

The categories are taken from the list of main categories associated with the selected Standard or diagram component questions. If multiple Standards are selected then this list is made up of the universal categories. Questions from a single Standard use the categories from that Standard.

### **Rank:**

The Rank column corresponds to the size of the bar on the chart and is an importance weighting.

For more information about how categories are ranked, see the [Category Rankings](#) help section.

### **Failed:**

The Failed Count shows the number of negative answers determined by either a No or Unanswered answer. The total number of questions does not include questions marked as not applicable.

### **Total:**

The Total indicates the total number of questions within the indicated category.

### **Percent:**

This column is the number of failed answers divided by the total number of questions to get the percentage.

The Overall Ranked Categories screen is shown in the Figure below.

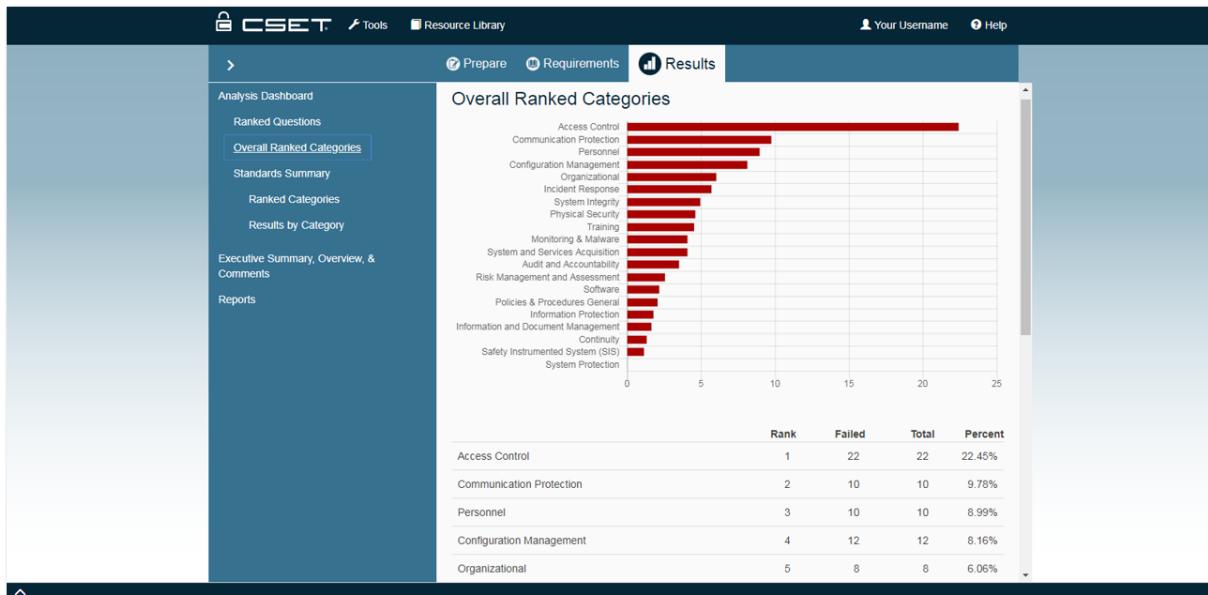


Figure: Overall Ranked Categories Screen

## Standards Analysis

The Standards Analysis section of the Analysis Navigation panel displays charts and tabular data based on answers to questions for the selected Standards. Standards Analysis contains analysis screens for Summary, Ranked Categories, and Results by Category that will be described in the following sections.

### Standards Summary

The Standards Summary Single Standard screen shows summary information related to the results from the answers to the single Standard that was selected at the Standards screen during the start of the assessment. The chart and tabular data displayed will correspond to a single Standard only.

The data displayed corresponds to answers to questions associated with only the selected Standard and does not include data related to components on the network diagram.

The chart shows the percentage of all Yes, No, NA, Alternate, and Unanswered questions for the selected Standard. The tabular data show the Answer in the first column. The second column indicates the number of the indicated answer, the third column shows the overall total number of questions, and the final column shows the percentage of the number for the total.

The Standards Summary Single Standard screen is shown in the Figure below.

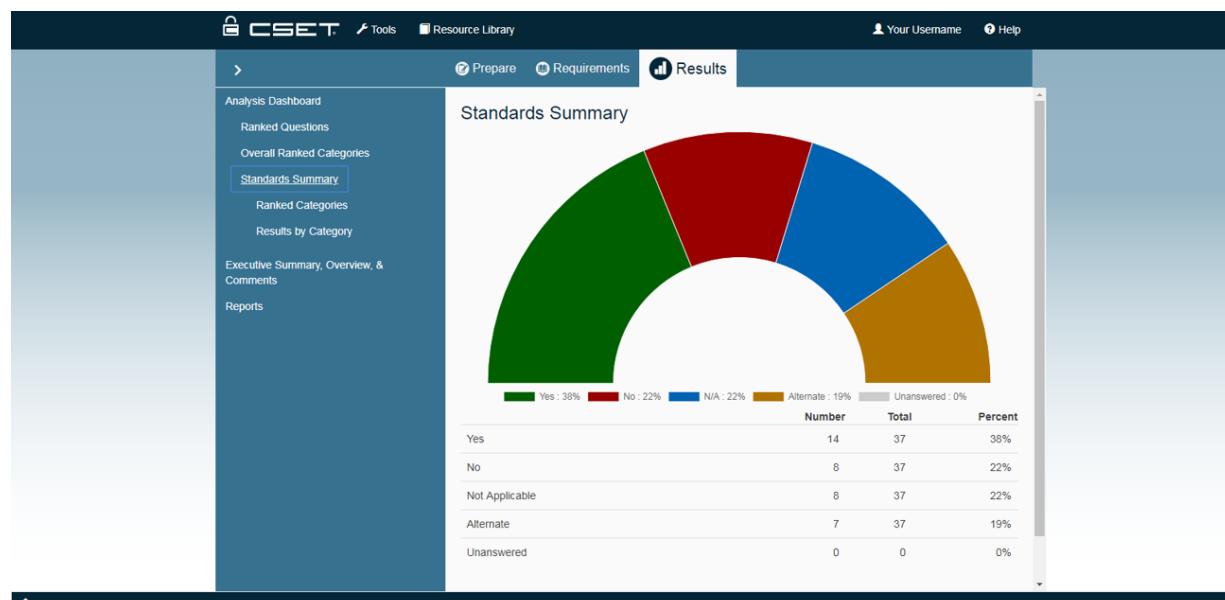


Figure: Standards Summary Single Standard Screen

## Standards Ranked Categories

The Standards Ranked Categories screen shows a list of all main categories ranked in order of the categories that should be prioritized based on how the questions were answered. Only answers from the selected Standards are included on this screen. Diagram component answers are not included. The chart shows the categories ranked in order of importance.

This screen highlights the categories that need the most attention for failed Standards based questions. Unlike other analysis screens that highlight the positive answers, this screen and the associated data show what categories or areas are weakest and what needs the most attention. In other words, the longer the bar in the chart, the worse the score in that area.

The Data Tab contains the tabular data of the categories that match the bars on the associated chart. There are five columns in the tabular data:

### **Category:**

The categories are taken from the list of categories associated with the selected Standards. If multiple Standards are selected then this list is made up of the universal categories. Questions from a single Standard use the categories from that Standard.

### **Rank:**

The Rank column corresponds to the size of the bar on the chart and is an importance weighting.

For more information about how categories are ranked, see the [Category Rankings](#) help section.

### **Failed:**

The Failed count shows the number of negative answers determined by either a No or Unanswered answer. The total number of questions does not include questions marked as not applicable.

### **Total:**

The Total indicates the total number of questions within the indicated category.

### **Percent:**

This column is the number of failed answers divided by the total number of questions to get the percentage.

The Standards Ranked Categories screen is shown in the Figure below.

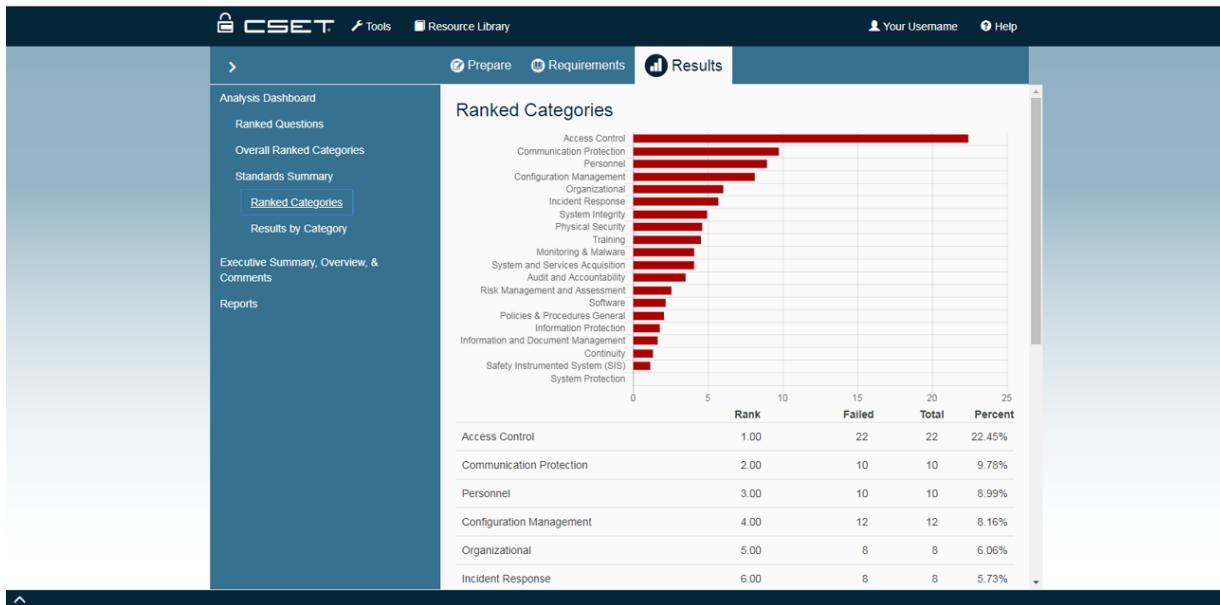


Figure: Standards Ranked Categories Screen

## Standards Results by Category Single Standard

The Standards Results by Category Single Standard screen shows the positive results of how the user performed on the assessment organized by the category in which the questions are grouped. The results are based on questions from a single Standard selected at the Standards screen during the start of the assessment. The chart and tabular data displayed will correspond to a single Standard only. If multiple Standards are selected, the [Standards Results By Category Multiple Standards](#) screen is displayed. The data displayed also do not include data related to components on the network diagram.

The chart displayed is a bar chart and shows the percentage of passed (Yes and Alternate) answers to questions for the selected Standard grouped into categories. The Data Tab shows the Category in the first column. The second column indicates the number of passed answers for the indicated category, the third column shows the total number of questions in the category, and the final column shows the percentage of the passed answers over the total.

The Standards Results by Category Single Standard screen is shown in the Figure below.

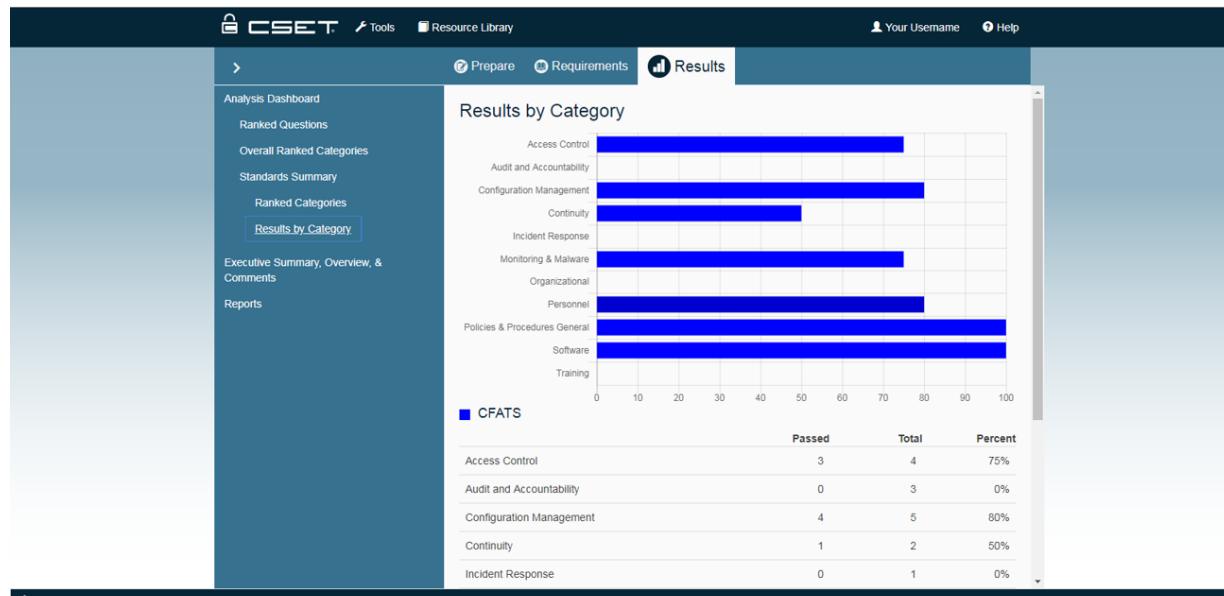


Figure: Standards Results by Category Single Standard Screen

## Standards Results by Category Multiple Standards

The Standards Results by Category Multiple Standards screen shows the positive results of how the user performed on the assessment organized by the selected Standards as well as the category in which the questions are grouped. The results are based on questions from multiple Standards selected at the Standards screen during the start of the assessment. The chart and tabular data displayed will correspond to multiple Standards. If a single Standard is selected, the [Standards Results By Category Single Standard](#) screen will be displayed. The data displayed also do not include data related to components on the network diagram.

The chart displayed is a multiple bar chart. For each category, the chart displays a bar for each selected Standard. Each bar shows the percentage of passed (Yes and Alternate) answers to questions for the indicated Standard. The Data Tab shows multiple tables, one for each Standard, with the Category as the first column. The second column indicates the number of passed answers for the indicated category, the third column shows the total number of questions in the category, and the final column shows the percentage of the passed answers over the total.

The main CSET window may need to be maximized in order to read the chart appropriately.

The Standards Results by Category Multiple Standards screen is shown in the Figure below.

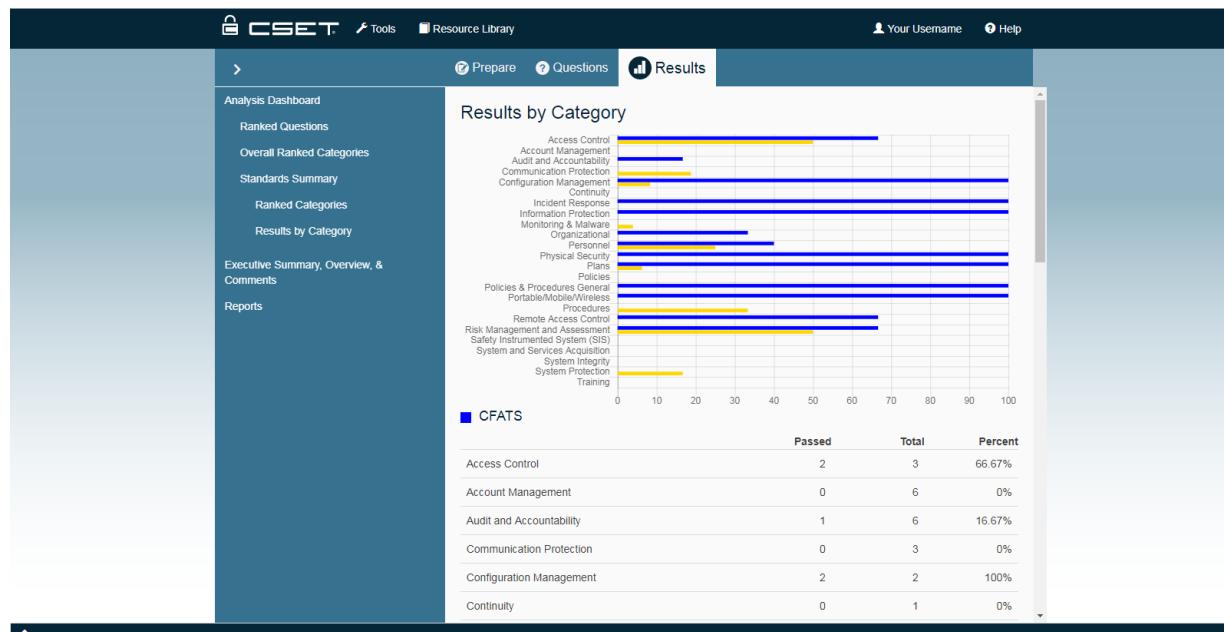


Figure: Standards Results by Category Multiple Standards Screen

## Category Rankings

Each Standard has an overall defined risk. This overall risk is determined from the number of questions and the weight of each question. The weights of questions have been determined by cyber security experts. If all questions have been completely failed then the ranked category bar charts will show that the user is at 100% of the risk defined by the Standard as seen in Figure: Ranked Categories with 0%. If about half the questions were answered yes, then the graph would only show the user at 50% of the overall risk as seen in Figure: Ranked Categories with 50%. See the two graphs below.

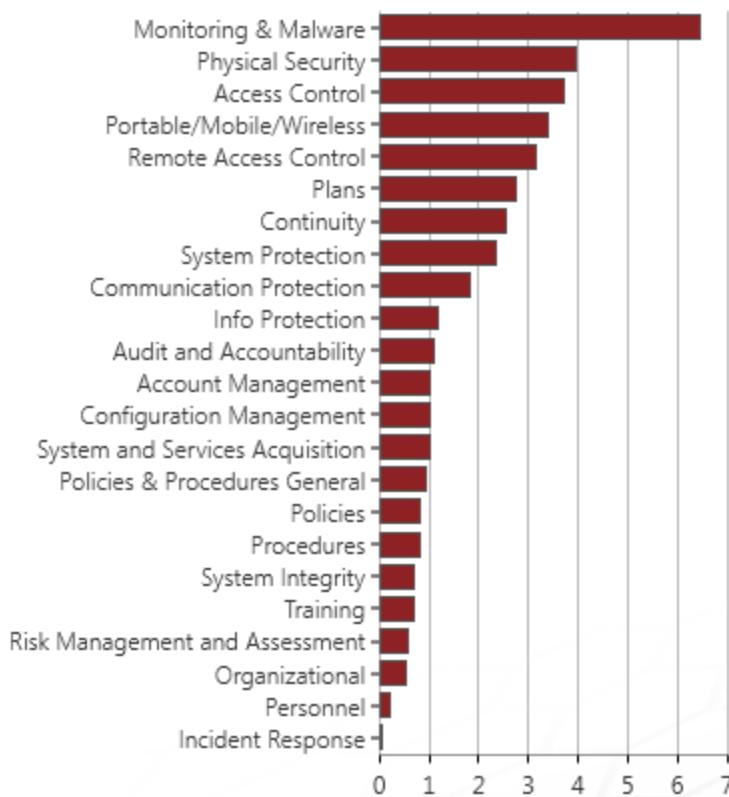


Figure: Ranked Categories with 0% of Account Management Questions Passed



**Figure: Ranked Categories with 50% of Account Management Questions Passed**

Note that the x-axis is different between Figures Ranked Categories with 0% and Ranked Categories with 50%. Otherwise the graphs look about the same. The x-axis changes because the proportions of risk are the same. According to this Standard, the Monitoring and Malware controls consume about 2/3 of the risk that Account Management does. However, if we go back and answer a great majority of Account Management questions as Yes then we obtain the chart in Figure: Ranked Categories with 100%.



**Figure 138. Ranked Categories with 100% of Account Management Questions Passed**

Now the risk accounted for from the Account Management section is only about 1% of the original risk defined by this Standard. Note that Monitoring and Malware still Accounts for about 6% of the overall risk as it did above.

## Reports Section

After the network diagram has been completed and both the Standards and component questions have been answered, the user can generate and print reports of the results.

The intent of the reporting function is to provide a way to print and publish assessment information, including summary charts and lists. It also provides a hardcopy of the results to be used in meetings, for communications to management, and as a way to assign tasks to technical staff. Combined with the online analysis, these reports can help the user clearly understand where weaknesses are and where improvements should be made.

This section will describe how to use the Reports Screen to select the report type, filter the content of the report, and then generate the report to different formats.

## Executive Summary, Overview, and Comments Screen

The Executive Summary, Overview, and Comments screen allows the user to add executive level information for display on the Executive Summary report. As well as, a high-level description of the assessment and any relevant comments to be displayed on the reports.

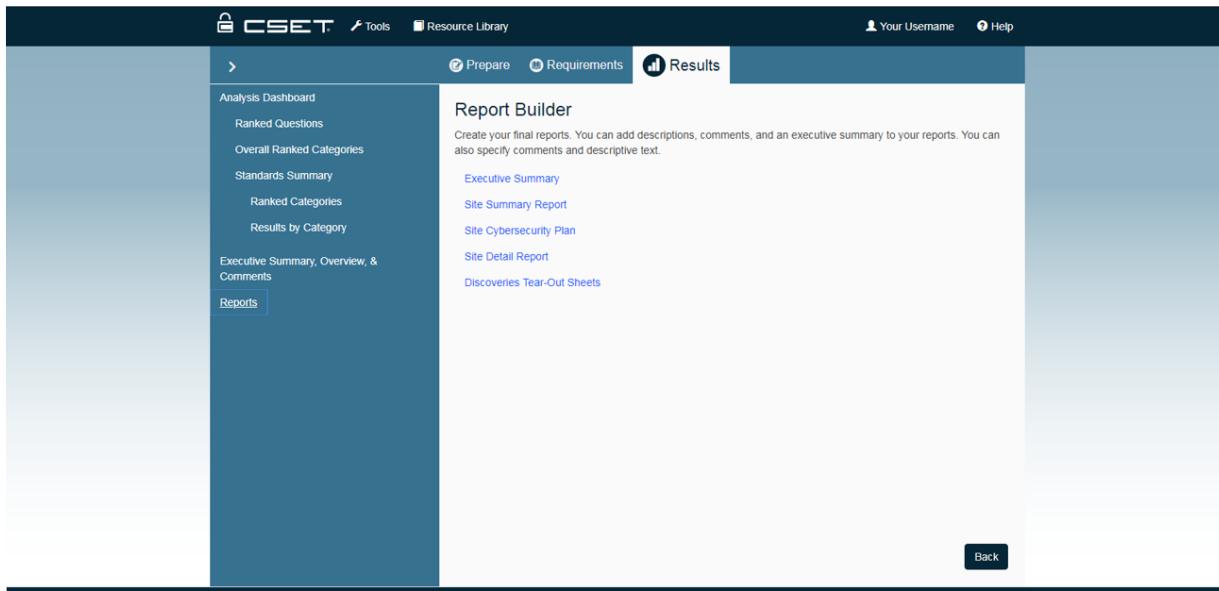
Some default text is provided on the Executive Summary screen; however, the user should replace that text with actual summary information that captures the highlights of the assessment as seen in the Figure below.

The screenshot shows the CSET software interface. At the top, there's a navigation bar with icons for 'Tools' and 'Resource Library', and a user account section with 'Your Username' and 'Help'. Below the navigation bar, the main menu has tabs: 'Prepare', 'Requirements', and 'Results'. The 'Results' tab is currently selected and highlighted in blue. On the left side, there's a sidebar with links: 'Analysis Dashboard', 'Ranked Questions', 'Overall Ranked Categories', 'Standards Summary', 'Ranked Categories', 'Results by Category', 'Executive Summary, Overview & Comments' (which is the active link, indicated by a blue border), and 'Reports'. The main content area is divided into three sections: 'Executive Summary', 'Overview', and 'Comments'. The 'Executive Summary' section contains a box of text: 'Cyber terrorism is a real and growing threat. Standards and guides have been developed, vetted, and widely accepted to assist with protection from cyber attacks. The Cyber Security Evaluation Tool (CSET) includes a selectable array of these standards for a tailored assessment of cyber vulnerabilities. Once the standards were selected and the resulting question sets answered, the CSET created a compliance summary, compiled variance statistics, ranked top areas of concern, and generated security recommendations.' The 'Overview' section contains a box of text: 'High Level Assessment Description: Please provide a description of the assessment process and work performed for senior management. This information will be included in your reports. This is not intended to be analysis of the assessment results as requested in the executive summary.' Below this, another box says: 'Please provide a description of the assessment process and work performed.' The 'Comments' section is currently empty.

Figure: Executive Summary Screen

## Report Builder

The Report Builder screen is shown in the Figure below. Notice that none of the options are checked when the screen is first accessed. The Create Report button is disabled until one or more reports and file types are selected. The Status bar will activate when the Create Report button is clicked to provide an indication of report creation progress. Reports can take a few seconds to many minutes to generate. The number of components contained in the network diagram will significantly impact report creation time.



**Figure: Report Builder Screen**

To generate a report click on the specific report link on the Report Builder screen. The report will open in a new tab.

**Executive Summary:** The Executive Summary option produces the Executive Summary Report. As the name implies, it is designed for an executive level audience. The person receiving the report may hold any title; however, the intent is to provide limited graphical and high-level, summary information that can be understood quickly.

This report is limited to around five or six pages and does not include any detailed information beyond listing the top categories and areas of concern. It includes the textual Executive Summary information available on the [Executive Summary Screen](#). It also includes the High Level Assessment Description, which is found on the [Comments & High Level Description screen](#).

**Site Summary:** The Site Summary option produces the Site Summary Report. The intended audience for this report is a technical manager or supervisor who is responsible for directing the implementation of the recommendations. The report includes everything in the Executive Report plus additional charts at a more detailed level. It also includes the network diagram and a list of all the questions in the assessment that were not positively answered. An important feature is the ranking of the missed questions. Each question is ranked sequentially.

from one to the total number of questions.

The question ranking is determined by a formula that takes into consideration the weighting of each question, the weighting of each category, and the security assurance level (SAL) associated with that question. All questions in CSET have been assigned a unique weighting relative to one another. The categories have been weighted as well. These assignments were determined by subject matter experts and are based on their recommendations. The SAL that is assigned to a question is also considered in the formula. For example, all other things being equal, if Question A has a SAL of High and Question B has a SAL of Low, then Question B would rank higher in the list than A. The recommended ranking would encourage addressing basic requirements before addressing the more difficult ones.

The rankings are intended to address the question, "What should I work on first?" It is recommended to start with the question ranked Number 1 and work down the list based on available resources and the cybersecurity plan.

**Detail Report:** This option will generate the Site Detail Report. The intended audience for this report is the implementers of change in the organization as it provides the details needed to make the necessary resource allocations and commitments to improve the cybersecurity of the facility or site.

**Security Plan:** The Security Plan option produces the Site Cyber Security Plan template. It provides an overview of system security requirements and describes the controls in place or planned to meet those requirements.

The plan includes several sections found in the Site Summary Report but the bulk of the report is a list of all assessment questions and their answers presented in a control-focused format. Thus, the report provides an overview of the cybersecurity requirements and the status for the facility.

**Discoveries Tear Out Sheets:** The Discoveries Tear Out Sheets option produces a list of all discoveries identified on specific questions during the assessment. Contacts can be assigned to each discovery record and the printed report will allow for easy distribution of assignments to address each discovery or potential issue.

## Executive Summary Report

The Executive Summary Report is designed for an executive level audience. The intent is to provide limited graphical and high level, summary information that can be understood quickly.

This report is limited to around five or six pages and does not include any detailed information beyond listing the top categories and areas of concern. It does include the textual Executive Summary and Description of Assessment text that was entered by the user at the Information screen. Some default text is provided; however, the default text should be replaced with actual summary information that captures the highlights of the assessment.

The Executive Summary Report has a fixed set of sections that are all generated when the report is created. Each of the sections in the report will be discussed below.

**Title Page:** Each of the reports has a cover page that is unique to the report type. Each includes the assessment name that is taken from the Information screen in the tool, the date that was entered in the Assessment Date field, and the name of the person that was entered in the Principal Assessor/Name field in the Information screen.

**Description and Summary:** This is the first page with content and shows a summary look at the Standards, network components, and overall compliance based on answers to questions in the assessment. It also includes the description of the assessment and the executive summary text that was entered in the Information screen.

When CSET is installed, the Executive Summary field has generic text included as a starting point; however, once the assessment is complete, the included text should be replaced with executive summary text that is specific to the actual assessment results.

**Standards Summary:** The Evaluation Against Selected Standards displays several items. It first identifies the Standards that were used in the evaluation. It then shows in pie chart format the combined breakout of answers for the selected Standards. The bar chart provides the greatest level of detail and indicates the overall scoring in each question category for the selected Standards.

Because more than one Standard may be selected, the categories are not specific to a single Standard. Instead, the categories are taken from a common list that applies to all.

**Areas of Concern:** The final section of the Report shows the top subjects or categories and top questions of concern.

The top questions and categories are based on the ranked order of both, and the full lists can be found in the Site Summary and the Site Detail reports. Both lists on this page have been limited to only the top five. The intent is to give a quick picture of what is recommended to be addressed first.

If the user selected the Requirements or Cybersecurity Framework approach to the assessment, this section will deal with the requirements of concern, and the list will be the actual requirement text.

**Ranking:** The list is based on a formula that includes the number of missed questions, the weighting given to each of those questions, the weighting assigned to the question category or area, the SAL for the question, and the criticality assignment for a component that was included in the diagram.

All the parameters are factored together. Each question is ordered in the list from the question the user should work on first at the top to the question or requirement that should be addressed last listed on the bottom.

## Site Summary Report

Selecting the Site Summary option produces the Site Summary Report. The intended audience for this report is a technical manager or supervisor who is responsible for directing the implementation of the recommendations. The report includes everything in the Executive Report plus additional charts at a more detailed level. It also includes the network diagram and a list of all the questions in the assessment that were not positively answered. An important feature is the ranking of the missed questions. Each question is ranked sequentially from one to the total number of questions.

The Site Summary Report provides mostly summary information in the form of a variety of charts; however, it is more detailed than the Executive Summary Report and provides additional charts that the Executive Summary Report does not have.

The sections of the Site Summary Report are discussed below.

**Title Page:** The Title Page includes the assessment name, date, and the name of the principal assessor.

**Disclaimer:** The disclaimer describes the limitations for use and legalities of CSET and the report.

**Advisory:** The Advisory includes recommendations for using CSET for more than an approach to a robust cybersecurity plan, for the team makeup, and for protecting data. It should be read and followed.

**Site Information:** This section displays the text that was entered on the Information screen in the tool. It will display all the data with the appropriate labels.

**Description and Summary:** This is identical to the first page of the Executive Summary Report.

**Standards Summary:** This page is identical to the page in the Executive Summary Report.

**Standards Compliance:** A Standards Compliance bar chart is displayed for every Standard selected in the tool. This chart gives the percent of positive answers (either marked as a Yes or Alternative) as compared with the total number of questions in each category. Unlike the earlier combined Standard Summary, this chart uses the categories that are specific to the Standard. The title on the chart is the short name or abbreviation of the full Standard name.

**Security Assurance Level (SAL):** The Security Assurance Level page displays the results of answers and selections related to the SAL. It includes any values that were determined in the General SAL or the FIPS 199 SAL processes along with any Standard specific values like those for DoD 8500.2. When Cybersecurity Framework Mode is selected as the assessment mode, this section will be changed to display the Cybersecurity Framework Tier Determination.

**Document Library:** The next page shows the document titles and file names of any documents that were added to the assessment by the user. They may have been added in association with specific questions or added through the Document Library screen.

**Ranked Subject Areas:** The Ranked Subject Areas section shows the categories or subject areas that need the most attention. This chart is organized so that the worst areas are shown at the top and then ordered to those areas doing best at the bottom. This chart can be helpful in prioritizing what areas to work on first.

The formula for ranking these areas includes several factors such as a weighting given to each area from subject matter experts combined with the number and level of missed questions in each area.

The top five areas shown on this chart are used to populate the top categories of concern section of the Executive Summary Report.

**Summary of Ranked Questions:** This table includes a list of the questions that were missed presented in ranked order. It makes up the bulk of the report. This list is intended to answer the question, "What do I work on first?"

The table also presents the SALs applicable to the question. General SALs will be listed for most Standards and network components. They are Low (L), Moderate (M), High (H), and Very High (VH). If a CNSSI Standard is selected, the Confidentiality (C), Integrity (I), and Availability (A) levels will be shown. If DoD Instruction 8500.2 is the selected Standard, the Confidentiality (Conf) and Mission Assurance Category (MAC) levels will be shown. They are: Classified (C), Sensitive (S), and Public (P) for Confidentiality; MAC I, II, and III for Mission Assurance Category.

For requirements mode, the table lists the name of the Standard and the available security levels.

The top five questions on this chart are used to populate the top questions of concern section of the Executive Summary Report.

The format of the table is:

Rank #	Question/Requirement Identifier	SAL
--------	---------------------------------	-----

Question or Requirement Text	Answer
------------------------------	--------

**Rank#:** The calculated position in the list.

**Question/Requirement Identifier:** The topic, category, or requirement and question number.

**SAL:** The SAL applicable to that question or requirement.

**Question or Requirement Text:** The text as seen in the Questions screen.

**Answer:** Why the question is listed in the table. Usually the question was answered No or left unanswered (blank). Unanswered questions should be reviewed and answered, then the report recreated.

**Ranking:** The list is based on a formula that includes the number of missed questions, the weighting given to each of those questions, the weighting assigned to the question category or area, the SAL for the question, and the criticality assignment for a component that was included in the diagram.

All the parameters are factored together. Each question is ordered in the list from the question the user should work on first at the top to the question or requirement that should be addressed last listed on the bottom.

The SAL of each question is included in the table which gives the user additional information when prioritizing work. A lower SAL usually means that the fix will be relatively simple. However, while more time consuming and costly to fix, a higher SAL, represents a higher level of protection. Resources should be allocated according to the calculated rank and the risk tolerance of the user.

**Question Comments/Marked for Review:** This section includes all the questions that had comments entered or had the Marked for Review check box clicked. It identifies the question by subject area and by number within the subject area and then displays the question, its answer, and the comment.

**Alternate Justifications:** This table is similar to the question comments table described above except that it provides the text that was entered as a justification for using an alternate method to accomplish the intent of the question.

## Site Detail Report

The Site Detail Report adds several new sections to the report that are not found in the Executive Summary or Site Summary Reports.

The following sections have been described in either the [Executive Summary Report](#) or the [Site Summary Report](#) help sections and will not be repeated here. To review the detailed description, please see the respective help section.

- Title Page;
- Disclaimer, Advisory, and Table of Contents;
- Assessment Information;
- Description and Summary;
- Standards Summary;
- Standards Compliance;
- Security Assurance Level (SAL);
- Document Library;
- Ranked Subject Areas;
- Summary of Ranked Questions;
- Question Comments/Marked for Review; and
- Alternate Justifications.

The new section added to the Site Detail Report is a list of the questions detail for each Standard.

**Question Details:** The final section of the report shows a full list of the questions that were asked and the answers that were given for the Standards. It identifies the question by subject area and by number within the subject area and then displays the question and its answer.

The questions are ordered based on the Standard or the Universal Set and are not ordered by ranking.

## Site Cyber Security Plan

The Site Cyber Security Plan provides an overview of the security requirements of the system and describes the controls in place or planned, for meeting those requirements. The Security Plan Report is presented in template format with some generic text (distinguished by being in 10 point font and italicized) that must be replaced with verbiage describing the actual site or facility and the assessment results. Sections to replace include:

- Signature Identification,
- Introduction,
- System identification,
- Roles and Responsibilities, and
- Risk Analysis.

**Security Assurance Level (SAL):** The SAL page displays the results of the answers and selections related to the SAL. When Cybersecurity Framework is selected as the Assessment Mode, this section will be changed to display the Cybersecurity Framework Tier Determination.

**Security Plan Controls and Status List:** This section lists all the requirements and controls selected during the assessment. The table includes the requirement title, the control description, affected zones and components, if there are any, and the related questions with the answers that were provided during the assessment. A brief description of each field is provided at the start of the section and repeated below.

**Requirement Title:** Is the control title as it is generally defined in the Standard document from which this control is derived.

**CSET Question/Requirement Category:** Shows the CSET Question category from the global questions list. Questions from multiple Standards have been consolidated together in the CSET tool and assigned a common category.

**Control Level:** Mapped to one of Low, Moderate, High, or Very High.

**Implementation Status:** Shows the percentage complete as the number of yes answers divided by the total related questions for this control. This percentage implemented will not necessarily be reflective of the amount of work required to implement the control but is merely an indicator of how many of the questions related to the control have been addressed so far.

**Short Standard Name:** Is an indicator of which Standard this control is derived.

**Control Description:** The full control text as defined in the Standard from which the control is derived.

**Related Questions and Answers:** A list of the questions and answers from which the implementation status of this control was determined.

The table is grouped by control, meaning that there may be several questions under each requirement. The table also summarizes the implementation status of each requirement as a

percentage of positive answers per number of related questions. It is ordered to match the on-screen display of the control questions so the user can more easily find and review requirements of interest.

This is the heart of the report. Using this table, the reader can quickly see all the requirements related to the facility and how closely each is being met.

## Cybersecurity Framework

When Cybersecurity Framework is selected as the Assessment Mode, the Security Plan Controls and Status List section will change to show information relevant to the Framework. The sections of the table will become as follows.

**Framework Function:** The high-level framework function indicating in which section of the framework the current control is defined.

**Control Category:** Shows the framework category from the global questions list.

**Implementation Status:** Same as described above.

**Control Description:** The full control text or subcategory as defined in the framework. They are the requirements or required actions.

## Discoveries Tear Out Sheets

Discovery records are identified and associated with individual questions during the assessment. As infrastructure or processes are evaluated during the assessment process, there are times when problems or issues are identified. These problems can be recorded and associated with the question under review. The Discoveries Tear Out Sheets contain a list of all Discovery records identified during the assessment. The report is formatted such that each discovery can be assigned to a person responsible for its resolution and easily assigned.

The Discoveries Tear Out Sheets report has a fixed set of sections that are all generated when the report is created. Each of the sections in the report will be discussed below.

**Title Page:** All reports have a cover page that is unique to the report type. The title page includes the assessment name taken from the Information screen in the tool, the date entered in the Assessment Date field, and the name of the person that was entered in the Principal Assessor on the Information screen.

**Disclaimer:** For information about the Disclaimer, see the [Disclaimer](#) help section.

**Advisory:** For information about the Advisory, see the [Advisory](#) help section.

**Table of Contents:** This is a system-generated table that indicates the report sections and the page numbers for those sections.

**Site Information:** This section displays the text entered on the Information screen in the CSET tool. It displays all entered data with the appropriate labels.

For more information about Site Information, see the [Site Information Screen](#) help section.

**Discovery List:** Provides a list of all Discoveries identified during the assessment along with the question associated to the Discovery.

For more information about Discovery records, see the [Discoveries Section](#) help section.

## Initiation Scenarios

The following initiation scenarios are provided as an overview of typical security vulnerabilities associated with shared control system and business system infrastructure or control systems connected to other external networks (hereafter any noncontrol system is referred to as an external network). It is intended that this information will stimulate thought and discussion for the team performing a CSET assessment, specifically, in determining a SAL. This overview is not intended to be a comprehensive review of all potential threats or vulnerabilities.

Three aspects must be considered when assessing the security posture of a control system:

**Availability.** The system must be ready and able to store and transmit data when needed.

**Integrity.** The data stored or transmitted by the system must be complete and correct (not corrupted).

**Confidentiality.** The system must be able to store and transmit data without unauthorized disclosure of sensitive information.

The following pages describe a typical ICS/external network environment and provide examples of risks, exposures, and vulnerabilities that are commonly encountered in such environments.

## Typical Mixed-Use Control/External Network Environment

In a typical mixed-use environment, there is separation between ICSs and external networks, but both rely on some amount of shared infrastructure (e.g., communications links). Although separated, some connectivity between these networks exists (e.g., public web or application servers).

There are typically distinct but interconnected networks, including the following:

**Control System.** The control system consists of servers, workstations, and devices associated with the ICSs. Multiple separate systems may be in use and individual systems may span multiple sites.

**Business Network.** The business network consists of servers and workstations associated with typical office productivity applications, such as email and word processing, as well as specialized applications such as for human resources, payroll, and billing.

**Other Networks.** These consist of other city, state, federal, or outside agency networks connected via dedicated communications, Virtual Private Networks (VPNs), or other means. Typically, access from such networks is controlled via a firewall. Connections to other networks may be trusted or untrusted.

**Internet.** For the public Internet, typically, access is allowed to the outside for business use (e.g., email, web browsing) and limited services may be accessed externally (e.g., web access to public information). Such access is controlled via a firewall, and the Internet is treated as an

untrusted network.

**Shared Infrastructure.** While the ICS and business environments are distinct, there are touch points between them.

Because of the costs and complexity associated with wide area networks, it is common to allow both ICS and normal business communications to share the same physical infrastructure.

The need to share information may drive the use of portals between networks in a dual-homed configuration with direct connection to both networks, or shared servers may be placed on a DMZ network between the ICS and the business.

ICS personnel with the need for business application access may be provided workstations that are dual-homed or provided access to the business network from their ICS workstations, or vice versa.

It is important to appreciate the complexity of ensuring security in such environments.

While individual products, systems, or networks may be secure when taken individually, they may not be adequately secured or protected in a complex deployment.

## Common Initiation Scenarios

The following scenarios describe common security issues that can initiate a worst-case scenario. The scenarios could impact the operation of a facility causing damage, loss of production, impacts to health, safety, and the environment, or other economic impacts. These issues could, in turn, impact system availability, integrity, and confidentiality in a typical mixed-use environment. These scenarios are provided as food for thought in developing an organization's worst-case scenario and the resulting consequences.

### Scenario 1: Privilege Escalation

In this scenario, an unknown party (attacker) is able to access sensitive data or systems by means of existing network connections. This access may be gained by a number of means, including:

**Insufficiently Protected Networks.** Restrictions between networks may be nonexistent, poorly implemented, or may rely on excessive levels of trust between networks.

**Privilege Escalation.** The outsider, or in some cases an insider, may access a public or loosely secured system with limited functionality and then use that system to hop to more sensitive functions. By hopping between systems, the attacker appears to be operating from inside the trusted network.

**Poorly Secured Resources.** A determined attacker can potentially exploit a number of system weaknesses, including but certainly not limited to the following:

- Unsecured Default Accounts. The attacker leverages widely known default accounts

and passwords to gain access.

- Poorly Secured Services. The attacker uses weaknesses in running services and applications to gain access to increased access levels (i.e., gaining access to sensitive system files).
- Weak Network Services. The attacker uses known vulnerabilities in services and applications to execute programs to gain further levels of access.

The attacker might proceed as follows:

- 1) Identifying the software running on the web server. While doing simple Internet searches, the attacker locates software capable of exploiting vulnerabilities within the web server software or the current configuration of the server to allow execution of programs on the web server.
- 2) Executing a remote shell (command prompt) on the web server to launch software identifying internal hosts. Upon discovery of an interesting server (the Control System Historian in this example), the attacker attempts to gain access using well-known default accounts (i.e., Guest), eventually discovering a little-used account with a default, or easily guessed password to gain access.
- 3) Using the trust associated with the control system Historian to gain access to the ICS network. In poorly secured systems, there may be excessive trust between inside servers and the ICS, which can allow easy access. Once in, the attacker uses additional probes to gain access to ICSs and to install software, view and manipulate data, or perform any other desired function.

Any such intrusion impacts the ICS network at multiple levels:

**Availability.** Through intentional or accidental reconfiguration, the attacker may disable essential system services, or introduce software (i.e., spam generators) that disrupts the network because of the traffic loads generated.

**Integrity.** Unauthorized manipulation of data can be done at the attacker's whim. This may range from simple curious tinkering to direct attempts to impact the ICS.

**Confidentiality.** Sensitive system functions may be identified, and data may be accessed and disseminated to unknown third parties.

## Scenario 2: Traffic Sniffing

In this scenario, shared network infrastructure (e.g., hubs, switches, routers) is used for both the ICS and business. An unauthorized user (attacker) on a non-ICS network is able to sniff network traffic and capture login credentials (username, password), sensitive data, and network information.

The attacker might proceed as follows:

- 1) In a direct attempt to sabotage the ICS, or simply out of curiosity, the attacker installs

packet capture (sniffer) software to monitor traffic on the network. This software is capable of capturing any visible traffic and may include the means to circumvent protection offered by switches. In an extreme case, the attacker can use man-in-the-middle attacks to circumvent encryption. Such software can be monitored in real time or simply run in the background to capture traffic of interest. In particular, user login IDs and passwords can be captured in this manner.

- 2) An authorized user eventually connects to the ICS using authentication credentials (username and password). Because of weaknesses in the application, the password is not encrypted or is encrypted using weak and easily circumvented techniques.
- 3) Having captured the login session, the attacker simply extracts the password from the network traffic stream (if clear text) or runs a password-cracking program against it (if encrypted). Once the user account details are known, the attacker is free to impersonate that user and gain access to the ICS.

Any such attack impacts the ICS network at multiple levels:

**Availability.** The attacker may intentionally or inadvertently disable the user account. Changes to device configurations may result in a loss of use.

**Integrity.** With access into the system, the attacker can make further attempts to use the same credentials on other systems. Unauthorized manipulation of data can be done at the attacker's whim. This may range from simple curious tinkering to directed attempts to impact the ICS.

**Confidentiality.** Once user credentials are compromised, the attacker may impersonate the user at will. Sensitive system functions may be identified, and data may be accessed and disseminated to unknown third parties.

### Scenario 3: Introduction of Malicious Software from Outside the System

In this scenario, a workstation used by an authorized user is compromised by means of malicious software, or malware such as Trojan horses, viruses, or worms (in any combination). Such software is typically written to allow the attacker to generate spam emails.

The sequence of events might occur as follows:

- 1) A user on an operator workstation with either connections into both networks (dual-homed) or an internal ICS workstation with access to the outside inadvertently downloads a program via an email attachment. Although most users know not to run programs from unknown outsiders, simple carelessness or a well-crafted social engineering message appearing to come from Network Support might convince them to launch the attached program. The program exploits vulnerability in the workstation operating system to install malware (a worm). Once installed, the worm begins replication thus filling the memory.
- 2) Eventually, the sheer volume of traffic generated by multiple copies of the worm running on the network overwhelms lower-speed Wide Area Network (WAN) links, resulting in loss of communications or a denial of service.

Any such attack impacts the ICS network at multiple levels, such as:

**Availability.** The most likely impact is network disruption due to the sheer volume of worm-related traffic (e.g., probes, spam, and bounce email messages.)

**Integrity.** Remote-control software allows the attacker unrestricted access to the compromised system. If the attacker has some means of accessing the system, unauthorized manipulation of data can be done at the attacker's whim. This may range from simple curious tinkering to directed attempts to impact the ICS.

**Confidentiality.** If remote-control software is installed, sensitive system functions may be identified and data accessed and disseminated to unknown third parties.

## Glossary

### Acronyms

Acronym	Definition
ALT	Alternate Method
C2M2	Cybersecurity Capability Maturity Model
CAG	Consensus Audit Guidelines
CCI	Control Correlation Identifier
CFATS	Chemical Facility Anti-Terrorism Standards
CFR	Code of Federal Regulations
CIP	Critical Infrastructure Protection
CIS	Center for Internet Security
CMMS	• Computerized Maintenance Management System
CNSSI	Committee on National Security Systems Instruction
CoR	Catalog of Recommendations
CSET	Cyber Security Evaluation Tool
CUI	Controlled Unclassified Information
DCS	Distributed Control System
DHS	U. S. Department of Homeland Security
DISA	Defense Information Systems Agency
DoD	U. S. Department of Defense
eMASS	Enterprise Mission Assurance Support Service
FIPS	Federal Information Processing Standards
HIPAA	Health Insurance Portability and Accountability Act of 1996
HMI	Human-Machine Interface
ICS	Industrial Control System
ICT	Information and Communications Technology
IDS	Intrusion Detection System
IIS	Internet Information Services
INGAA	Interstate Natural Gas Association of America
IR	Interagency Report
IT	Information Technology
MAC	Mission Assurance Category

MIL	Maturity Indicator Level
MSC	Multiple Services Component
NA	Not Applicable
NEI	Nuclear Energy Institute
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
PCIDSS	Payment Card Industry Data Security Standard
PDF	Portable Document Format
PII	Personally Identifiable Information
PLC	Programmable Logic Controller
RBPS	Risk-Based Performance Standards
RG	Regulatory Guidelines
SAL	Security Assurance Level
SCADA	Supervisory Control and Data Acquisition
SP800	Special Publication 800
TSA	Transportation Security Administration
URL	Uniform Resource Locator
USB	Universal Serial Bus
VPN	Virtual Private Network

## Key Terms

Term	Explanation
Admin Questions	Questions spawned by the tool in response to the applied Standards the user selects.
Assessment Documents	Repository of documents added to the assessment by the user.
Assessment Report	A summary report of results for each question including user responses, statement of actual requirements (or deficiencies), answers in relation to the overall SAL, and associated help documents.

Classified Information	Any information or material that has been determined by the U.S. Government pursuant to an executive order, statute, or regulation, to require protection against unauthorized disclosure for reasons of national security (Classified Information Procedures Act, 18 U.S. Code App. 3, Section 1(a)).
Component Diagram or Network Diagram	A network topology that best represents the industrial control system configuration. Diagram includes typical components associated with a control system such as connector, firewall, network router, network switch, serial switch, network hub, modem, programmable logic controller, remote terminal unit, HMI, engineering workstation, intrusion detection system, wireless access point, serial radio, application server, database server, terminal server, web server, virtual private network, link encryption, DCS, printer, and clock.
Component Questions	A generated list of control system cybersecurity questions based on the defined SAL and components contained within the network topology diagram.
Confidentiality Level	Applicable to DoD information systems, the confidentiality level is primarily used to establish acceptable access factors, such as requirements for individual security clearances or background investigations, access approvals, and need-to-know determinations; interconnection controls and approvals; and acceptable methods by which users may access the system (e.g., intranet, Internet, wireless). The DoD has three defined confidentiality levels: classified, sensitive, and public.
Critical Asset	Those facilities, systems, and equipment, which if destroyed, damaged, degraded, or otherwise rendered unavailable, would have a significant impact on the ability to serve large quantities of customers for an extended period of time, would have a detrimental impact on the reliability or operability of the electric grid, or would cause significant risk to public health and safety.
Mission Assurance Category	Applicable to DoD information systems, the mission assurance category reflects the importance of information relative to the achievement of DoD goals and objectives. Mission assurance categories are primarily used to determine the requirements for availability and integrity. The DoD has three defined mission assurance categories: MAC I, MAC II, and MAC III. MAC I systems require the most stringent protection measures.
Public Information	Official information that has been reviewed and approved for public release by the information owner.
Resource Library	Electronic copies of cybersecurity documentation are included in the tool for reference, including federal codes, white papers, reports, industry Standards, and guidelines.

Security Assurance Level	<p>The relative consequences of a successful attack against the control system being evaluated. The consequence analysis identifies the worst, reasonable consequence that could be generated by a specific threat scenario. The General SAL provides an overall rating of the criticality based on the users' review of security threat scenarios and estimated consequences.</p> <p>The SAL ranges from Low to Very High.</p>
Security Categories	<p>The security categories are related to the NIST 800-53 Standards and are defined as:</p> <p><b>CONFIDENTIALITY</b> “Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information...” A loss of confidentiality is the unauthorized disclosure of information.</p> <p><b>INTEGRITY</b> “Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity...” A loss of integrity is the unauthorized modification or destruction of information.</p> <p><b>AVAILABILITY</b> “Ensuring timely and reliable access to and use of information...” A loss of availability is the disruption of access to or use of information or an information system.</p>

Security Categorization	<p>The NIST 800-53-related security categorizations of Low, Moderate, and High are explained as:</p> <p><b>LOW:</b></p> <p>The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.</p> <p><b>AMPLIFICATION:</b> A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.</p> <p><b>MODERATE:</b></p> <p>The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.</p> <p><b>AMPLIFICATION:</b> A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.</p> <p><b>HIGH:</b></p> <p>The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.</p> <p><b>AMPLIFICATION:</b> A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.</p>
Security Level	The rating of High, Moderate, or Low for Confidentiality, Integrity, and Availability according to FIPS 199 and NIST SP800-60.

Sensitive Information	Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an executive order or an act of Congress to be kept secret in the interest of national defense or foreign policy.
-----------------------	---

## Frequently Asked Questions (FAQs)

This is a list of questions that new users may find helpful.

### **My system is running slow. How can I make it go faster?**

This release may run slower than previous releases of CSET. Check to make sure that there is sufficient RAM on the user's computer. 3 GB of RAM is recommended. Check the Task Manager to verify that the computer is not paging to the disk drive, which would cause a significant drop in performance. The delays typically come from the system loading and caching data between the main screens. There is a greater delay when using a large diagram or when multiple Standards are selected. A faster processor will also help.

### **How do I import a file from a previous release of CSET?**

See [Import a CSET Assessment](#) for more information.

### **Why isn't the Catalog of Recommendations available in Questions mode on the Standards screen?**

The Catalog of Recommendations, Version 7 was the foundation for the Universal Questions and so to select it would be to double-select the same set of questions. To avoid confusion, it is not selectable in Questions mode.

### **What Standard should I use?**

Only the user can answer that question for his or her organization; however, extensive help information can be found by reviewing the [Cybersecurity Standard Selection](#) help section. The user may also consult the User Guide available from the Home screen. For a brief description of the available Standards, see the [CSET Standards and Question Groupings](#) help section.

### **Can I unclick an answer in the Questions screen after making a selection?**

Yes. Simply click the radio button again to clear it.

### **The video tutorials will not open.**

With CSET Version 6.0 and later, the tutorial videos were redesigned to play in YouTube. Therefore, an active Internet connection and suitable internet browser are required to view them. CSET will provide the web address or URL. The user must copy it and paste the URL into the Internet browser address bar. If the web address provided by CSET does not work, try opening YouTube ([www.youtube.com](http://www.youtube.com)) separately then searching on "Cyber Security Evaluation

Tool." Searching on "CSET" alone may not provide the desired results.

Internet connections with low bandwidth can result in reduced video quality.

To view closed captioning in YouTube click on the cc icon.

## CSET Revision History

<b>Document Revision</b>	<b>Date</b>	<b>Change Description</b>
0	August 2009	Initial release
1.0	April 2010	Updated Regulatory Basis in Section 2. Added instructions for new functionality in the drawing tool.
1.1	May 2010	Added need for Word 2007 to support RTF report. Revised description of component diagram zones.
2.0	August 2010	Updated Regulatory Basis in Section 2. Added instructions for new navigation and user interface.
3.0	July 2011	Updated Regulatory Basis in Section 2. Added instructions for the resource library, diagram layering, line security, and new report format.
4.0	January 2012	Updated the component diagram section to explain the use of Microsoft Visio.
5.0	December 2012	New architectural change to .NET and new approach with questions and requirements. New diagramming tool and system redesign for ease of use. Added new standards and modified default approach for component questions. Added new analysis capabilities and enhance resource library.
5.1	June 2013	Modifications to the Questions screen with headings, new standards, and modifications to standards and analysis to accommodate the CNSSI baseline and overlay.
6.0	January 2014	Added aggregation functionality and new standards, modified the diagram interface to improve usability, added the ability to create a component inventory list from the diagram, and added new Security Plan Report option. Video tutorials were moved to YouTube for online viewing.
6.1	July 2014	Added new Cybersecurity Framework mode to the standards options, revised the Analysis function to include Framework details, and modified the Network Diagram tool to improve how Zones are used and to clarify tab and menu names.

6.2	January 2015	Added fields for the Real Property and Site Unique Identification (RDSUID) information, added a new Security Assurance Level (SAL) determination for CNSS, added functionality to import information pertaining to the network diagram from Grass Marlin, added functionality to export information pertaining to eMASS, and added two new standards.
7.0	August 2015	Implemented a new, more modern design for the tool. Increased responsiveness of the Questions and Diagram screens. Added Cybersecurity Capability Maturity Model (C2M2), DoD Instruction 8510.01, and NISTIR 7628 Volume 1, Revision 1 as new standards.
7.1	January 2016	Added 43 new components to the diagram including new radio and medical components. Added ability to change parameter values on requirement text. Redesigned the analysis screens and added NERC Rev. 5 Compliance analysis capability. Added NIST SP800-161 Supply Chain Risk Management. Deprecated CNSSI 1253 Baseline and Overlay Standards.
8.0	September 2016	Redesigned the overall process to streamline the Preparation, Assessment, and Results processes and make the CSET tool easier to use by novice users. Added the ability to create custom questionnaires or custom question sets from any of the existing standard questions. Added the following Standards: Control Correlation Identifier Specification V2 Release 0.1, Critical Security Controls Version 6, Health Insurance Portability and Accountability Act Security Rule and NIST Special Publication 800-171. Added ability to collect discoveries on questions. Added four new components/symbols to the diagram.
8.1	February 2018	Fixed several application errors and started adding basic accessibility functionality to address 508 requirements.
9.0	October 2018	Moved to a web application with mobile capabilities.