**Cyber Security Evaluation Tool (CSET)**

**Technical Release Notes**

**An Explanation of Features and Enhancements**

**CSET Release Dates**

The following table provides the key dates for the release and distribution of the CSET application. The Release Date is when CSET development and testing was completed and the software released for use. The Estimated Distribution Date is the approximate date that the software was made available for download through the Department of Homeland Security (DHS) webpage.

|  |  |  |
| --- | --- | --- |
| **CSET Version** | **Release Date** | **Estimated Distribution Date** |
| 1.0 | August 2009 | September 2009 |
| 2.0 | April 2010 | May 2010 |
| 3.0 | August 2010 | September 2010 |
| 4.0 | August 2011 | September 2011 |
| 4.0.1 | December 2011 | December 2011 |
| 4.1 | January 2012 | February 2012 |
| 5.0 | December 2012 | January 2012 |
| 5.1 | May 2013 | June 2013 |
| 6.0 | February 04, 2014 | February 27, 2014 |
| 6.1 | July 2014 | August 7, 2014 |
|  |  |  |

**CSET Release Notes:**

CSET Version 6.1:

Version 6.1 included the addition of the Cybersecurity Framework as an assessment mode. The network diagram was revised to more easily incorporate zones.

* The following standards were added:
  + Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, National Institute of Standards, February 12, 2014

**Enhancements include:**

* The inclusion of the Cybersecurity Framework resulted in changes to the Standards screens to permit selection of Tiers and the creation of Profiles. Profiles are used to form and manage question sets tailored to the specific needs of a business or facility. Profiles can reflect the current security posture or can be used to set cybersecurity goals.

Changes were also made to the Question screen to accommodate the display of questions and requirements related to Framework activities. The Analysis screens were updated to provide detailed on-line summary information on the results on an assessment using the Framework mode.

* The Network Diagram was improved by making the Zone icon easier to access. The inclusion of shapes, components, and lines into a new Zone is now more intuitive.
* Several tab and menu labels were revised within the Network Diagram function to improve clarity.

**Issues:**

* Some anti-virus software programs have been found to significantly slow the download and installation of CSET from the DHS website.
  + An installation disk may be requested from DHS if this is a problem.
* If using the Windows Vista operating system, Microsoft .NET Framework 4.5 Full Runtime must be installed manually prior to installing CSET.

CSET Version 6.0:

Version 6.0 included the addition of the aggregation functionality. The diagram interface was modified to improve usability. The ability to create a component inventory list from the diagram was added as was a new Security Plan Report option. The video tutorials were moved to YouTube for on-line viewing.

* The following standards were added:
  + NEI 08-09 Cyber Security Plan for Nuclear Power Reactors
  + NISTIR 7628, Guidelines for Smart Grid Cyber Security, Vol 1
  + INGAA Control Systems Cyber Security Guidelines for the Natural Gas Pipeline Industry
  + NIST Special Publication 800-53, Rev 4, Appendix J
  + NIST Special Publication 800-82, Rev 1
  + CNSSI No. 1253 (ICS) Overlay Version 1

**Enhancements include**:

* The ability to work with more than one assessment at once was added. It is called Aggregation. There are three types of aggregation as discussed below: Trend, Compare, and Merge. The analysis result of Trend and Compare is a report. The result of the Merge function is a new assessment.
  + Trend shows cumulative changes to a facility over time by analyzing several assessments of the same facility completed, say, annually. Analysis results include a display of the overall compliance by percent ranged over the time period covered by the loaded assessments, compliance of each assessment by security area, and the top five most and least improved security topic areas.
  + Compare looks at multiple assessments to determine their strengths and weaknesses and creates a summary compliance report. This would be helpful for a facility consisting of several sites, each with their own completed assessment. Analysis results include an overall compliance summary by standard and component answers and broken out by security area, a list of commonly missed questions, a comparison of compliance by the individual assessments by standard and component answers and by security area, and a display of the percent of each answer option by assessment and security area ordered as best to worst compliance.
  + Merge joins several partial assessment files into a cohesive whole in the case where, for example, members of the assessment team were each assigned a portion of the assessment and each created an incomplete or partial assessment file. Choosing this option creates a new, single assessment file which can be opened and edited in CSET.
* Usability of the network diagram interface was improved by streamlining the drawing and editing tools. Adding a Zone box was made more intuitive.
* The ability to create a component inventory list from the diagram components was added. The list opens in Microsoft Excel where it is fully editable. The list can also be included in some of the printable reports.
* A new printable report option was added. It is called a Security Plan and is formatted as a template with example text to aid the user in addressing relevant security topics. It provides an overview of the security requirements of the assessed system and describes the controls in place or planned for meeting those requirements. The control list is grouped by security control.
* Access to the video tutorials was changed from a large download to viewing on YouTube. The videos are still context-specific meaning that if accessed from a particular screen, the video will discuss that screen, but all the videos are available for viewing at any time. An active Internet connection and web browser are needed to open YouTube. This resolves the video issue noted for CSET Release 5.1.

**Issues:**

* When opening a CSET assessment, diagram, or aggregation file received via email or the internet, it may fail to function if the temporary folder assigned by the email or internet application becomes locked or is removed. This happens because files attached to emails are often stored in a Temp folder which is deleted or locked when the email application is closed. If a CSET file is open in CSET when the email application is closed and the Temp folder deleted, the CSET file can become corrupted and unusable.
  + The issue can be prevented by downloading and saving the CSET file to a new location before opening it in CSET.
* Occasionally the PDF version of the Executive Summary report will have spurious line spaces in the Top 5 List.
  + The issue can be resolved by creating a DOCX version of the report and saving it to a PDF format.

CSET Version 5.1:

The Questions screen was modified to add headings. New standards were added. The standards and analysis functions were modified to accommodate the CNSSI baseline and overlay.

**Issues:**

1. There is a known issue related to the H.264 codec that CSET uses to display the video tutorials. It is related to the MP4 wrapper on the Windows Presentation Foundation (WPF) 4.0 media element.

This issue is manifest when trying to play the videos on a secondary monitor. When attempting to drag the video player across to the second monitor the player will lockup or crash. CSET has programmed the player to remain in the primary monitor only. For more information see comments from Microsoft at:

<http://social.msdn.microsoft.com/Forums/en‐US/wpf/thread/75d72afa‐2fff‐44fd‐9f0a‐87753002daa1/>

1. There is a known issue in the .NET Framework that affects the CSET application. CSET 5.1 may crash while opening the questions screen. If this occurs you can resolve the issue by getting the latest updates for the .NET Framework through Windows Update.

CSET Version 5.0:

CSET Version 5.0 incorporates a major architectural change to .NET framework. A new approach to questions and requirements was implemented. Diagramming was changed to use a diagramming tool and redesigned for ease of use. New standards were added and the default approach to component questions was modified. New analysis capabilities were added and the resource library was enhanced.

**Issues:** None

CSET Version 4.1:

CSET Version 4.1 provides users with the option of creating or modifying their network diagram in Microsoft Visio. The CSETVisio add-on was created to supply a new Visio stencil with network shapes recognized by CSET. CSET takes the Visio diagram and assigns questions to the included components and looks for network vulnerabilities as if the diagram had been created within CSET using DrawNodes.

**Issues:**

* Searching the resource library with double quoted strings returns some spurious results.

CSET Version 4.0.1:

CSET Version 4.0.1 is a minor release to address an issue related to how the tool used network diagram zones to calculate compliance of the components within the zone. Additionally, the release was used as an opportunity to improve several aspects of the tool.

**Enhancements include**:

* A new sub-report was created to display user-added comments.
* The PDF report was improved to better display question text.
* The look of the report title page was improved.
* Fields for user entered text were resized to better match the space allocated in the printed reports.
* The gap analysis in the question detail screen was revised to show the required answers in the same order as they appear in the questionnaire.
* Consistency between the Site Summary and Detail reports was improved.

**Issues**: None

CSET Version 4.0:

CSET Version 4.0 incorporates major improvements to the assessment reports, a new resource library, and additional diagramming capabilities. New standard question sets were added and several question sets were updated.

**Enhancements include**:

* The Option screen was redesigned to group standards of similar focus to improve ease of selection.
* The following question sets were added:
  + Catalog of Security Recommendations (CoR), version 7,
  + North American Electric Reliability Council (NERC) Critical Infrastructure Protection (CIP), rev 3,
  + Key Requirements Evaluation,
  + US Nuclear Regulatory Commission (NRC) Regulatory Guide 5.71, and
  + Chemical Facility Anti-Terrorism Standards (CFATS) Risk-Based Performance Standards (RBPS) Guidance, standard 8, “Cyber.”
* The outdated CoR V. 4 (Global 2009), NIST SP800-53 Rev 2 and Rev 3 Final Public Draft, and NERC CIP Rev 1 questionnaires were removed from the tool to keep the question sets relevant to current standards.
* A new questionnaire called Key Requirements Evaluation, was created to assist users who have limited time available for an assessment. With less than 100 questions, this questionnaire focuses on the most important concepts in cyber security.
* A resource library was added to the tool. It contains multiple reference documents including the standards used in the tool, guidelines, white papers, and templates chosen to provide additional assistance to users. A search feature is included to facilitate finding specific documents or topics of interest.
* The network diagramming function was improved to include layering and line security. Layering allows network components to be assigned to levels or tiers which can be displayed and analyzed or temporarily ignored by the tool. Line security allows designation of untrusted links between components.
* The assessment report interface was redesigned to more closely match the look and feel of other sections of the tool.
* Three new report options were added. Current report formats available are:
  + The Executive Report focusing on summary graphics,
  + The Site Summary Report providing additional detail,
  + The Detail Report ( the original printed report) containing user-selected sub-reports , and
  + The Enterprise Evaluation Report spotlighting business system compliance.
* The gap analysis portion of the reporting function was separated onto its own screen.
* The tool was adapted to operate in a 64-bit Windows 7 environment.

**Issues**: None

CSET Version 3.0:

CSET Version 3.0 incorporates an improved user interface that provides increased guidance for new users while allowing experienced users to interact with the system in their accustomed manner. New standard question sets were added and several question sets were updated.

**Enhancements include**:

* Guidance was enhanced to improve user understanding. The Options screen, where users select the standards to apply to their assessment, now includes mouse-over help, context sensitive help, and information on the purpose and use of each standard.
* Overall tool navigation was improved to allow new users to walk through their selected question sets in the order recommended by the tool and with guidance text at the start of each new standard.
* The navigation tree was enhanced to show the collected content of all the tabs and question sets instead of just the currently visible question set.
* Question detail screens were linked to each question in the questionnaires. They show the question, supplemental guidance, the level-specific requirement, links to source documents and help documents, and a gap analysis for that question and the selected answer.
* A group of icons was added to each question screen to access context sensitive guidance, the related video tutorial, the user guide, and the document library.
* Question sets were added for NIST SP800-53 Revision 3 with Appendix I, Catalog of Security Recommendations, version 6, and Consensus Audit Guidelines (CAG) version 2.3. The outdated Global Assessment 2008 questionnaire was removed from the tool to keep pace with more current standards.
* The tool's menu options were simplified by moving the component diagram options onto the component diagram screen.
* The assessment report screen was modified for easier viewing. The question details were linked to a new pop-up screen to reduce the length of the on-line report.

**Issues**: None

CSET Version 2.0:

CSET Version 2.0 was created to incorporate additional standards and to enhance the functionality of the component drawing tool.

**Enhancements include**:

* The creation of Rich Text Format (RTF) reports was improved for large amounts of printed data, which addresses the issue seen in the previous version of CSET. The RTF reports can be displayed in most word processing software to allow the user to revise the report text as desired.
* Question sets were added for NIST SP800-53 Revision 3 (Final) and NERC CIP-002 through CIP‑009, Revision 2 standards. The outdated NIST SP800-53 Revision 0 and Revision 1 standards were removed from the tool to keep pace with more current standards and to reduce user interface clutter.
* The drawing tool was improved to include the creation of zones. Zones identify a group of components that share the same Security Assurance Level (SAL), where the SAL can be lower than the plant SAL.
* The drawing tool now automatically checks for network deficiencies such as missing firewalls, missing IDS or IPS components, or components with interfaces to subnets at different security levels. Flags are added to the diagram to indicate the potential deficiency and can be used to access a text‑based description of the deficiency.

**Issues**: None

CSET (Version 1.0):

The initial version of the Cyber Security Evaluation Tool (CSET) has its foundations in Version 2.1 of the Control System Cyber Security Self-Assessment Tool (CS2SAT) and the Cyber Security Vulnerability Assessment (CSVA) tool. CSET combines the best attributes of both for a more comprehensive assessment.

**Enhancements include**:

* Requirements from the Catalog of Control Systems Security: Recommendations for Standards Developers were added to the tool under the tab labeled Global. CSET includes Global 2008 and the newly created 2009 versions. Previously known as COR, these requirements present a compilation of practices that various industry bodies have recommended to increase the security of control systems from both physical and cyber attacks.
* Question sets were added for NIST SP800-53 Revision 3 (Final Public Draft) and NIST SP800-82, Revision 0 standards.
* The drawing tool was improved to include component labeling. The attributes of the text (character, size, bold, etc.) may be modified by the user. Other drawing tool improvements include the addition of “Snap to Grid” functionality and size adjustment to allow the diagram to be printed on multiple paper sizes.
* Functionality previously found in the CSVA tool for business cyber systems was incorporated into CSET. This allows the user to complete a vulnerability assessment on ten key areas based on international, audit community, and federal government standards and guidelines. The related printed report sections present assessment results ordered by vulnerability severity.
* CSET now provides two options to the user to determine the security levels associated with all revisions of NIST SP800-53 and the Global Assessments. If the user is familiar with NIST SP800-60 and FIPS 199 criteria, he/she may assign the Confidentiality, Integrity, and Availability levels directly. Otherwise, a new questions set will be spawned to guide the user through a series of questions developed to calculate the security levels. The user may override the calculated levels if desired.
* Standards mapping has been introduced in CSET. This allows the user to transfer the answers from one standard to another if the question and answer sets are comparable between the standards. Significant time and effort will be saved by the user not having to answer the same questions multiple times when completing questions from similar standards or multiple revisions of the same standard.

**Issues**:

* Large reports created in Rich Text Format (RTF) may not display correctly in Microsoft Word. It is recommended that smaller sub-reports be created instead of one large report. The problem is seen in reports larger than about 400 pages.

CS2SAT Version 2.1:

Version 2.1 of the Control System Cyber Security Self-Assessment Tool (CS2SAT) was created to incorporate new standards and to improve the user interface.

**Enhancements include**:

* Requirements from the Catalog of Control Systems Security: Recommendations for Standards Developers were added to the tool under the tab labeled Global. Also known as COR, these requirements present a compilation of practices that various industry bodies have recommended to increase the security of control systems from both physical and cyber attacks. The requirement set is not limited for use by a specific industry sector but designed to be of benefit to any industry using control systems.
* The drawing tool was improved to include a cloud icon. This represents the internet external to the intranet. It behaves as a terminator; that is, subnet changes are not passed to other links through the cloud component. The default label is Web, but this may be changed by the user.
* The ability to add free-form text to the diagram for component labeling was added.
* In the case where a second component is added to the component diagram, the answers supplied for the first component of that type may be automatically copied to the second component. The user is given the option to copy the answers or not. The user may always override copied answers to better tailor the answers associated with an individual component.
* The components in the left-panel question tree are now displayed in alphabetical order for easier user navigation.
* The printed report was improved. The assessment title is now displayed on the title page of the report, and the report includes a table of contents. Users may compose an executive summary for inclusion in the printed report. If comments were added to a question, those comments will be displayed in the report regardless of whether the question was answered. The option to add a PCII banner to the header and footer of the report was added. The PCII banner displays: “Protected Critical Infrastructure Information.”
* The tool now performs an autosave at 15-minute intervals. This provides protection against data loss should a power failure or other incident suddenly close the tool.
* Text display was improved in several dialog boxes and menu items. Further, opening an existing assessment now returns the user to the tab and questions displayed when the tool last exited.

**Corrected known issues**:

1. The check box in the Edit menu that allowed the user to display the question identifier numbers was not consistently displayed.
2. Placing a forward or back slash in the assessment name caused problems with the diagram tool. This was corrected by automatically changing the slash to a dash for the drawing filename.
3. If the user dragged the tool frame, successive frames appeared and the tool response was slowed. This was corrected so that the tool responds in a timely fashion after a resize of the frame.

**Issues**:

1. Large reports created in Rich Text Format (RTF) may not display correctly in Microsoft Word. It is recommended that smaller sub-reports be created instead of one large report. The problem is seen in reports larger than about 400 pages.

CS2SAT Version 2.0:

Version 2.0 was created to incorporate additional standards and to improve functionality.

**Enhancements include**:

* The SANS Top 20 requirements for 2005 were rewritten. The SANS Top 20 requirements for 2006 and 2007 were added along with response options. The three SANS Top 20 question sets were reprogrammed as individually selectable.
* The NIST SP800-53 was expanded to include Revision 1 and Revision 2. Requirements were translated into question sets with response options. The user interface was reprogrammed to allow separate selection of Revisions 0, 1, and 2. FIPS 199 category selection was integrated into the NIST question sets to better tailor the focus of the assessment. Functionality was added to appropriate NIST questions to allow downgrading of the security category for just that question. Finally, NIST SPP-CIPCS links were removed.
* The SAL questions tab is keyed off of the standards chosen by the user. It is only displayed when the appropriate standard(s) is selected.
* Access to the diagramming tool was improved and the user options clarified.
* The drawing tool was improved to include additional components such as an Intelligent Electronic Device (IED), Master Terminal Unit (MTU), and a Front End Processor (FEP). The printer was changed to a network printer. Two VLAN components were added to allow assignment of multiple subnets. For each of the new components, requirements were investigated, a question set with response options was generated, and a new icon was created.
* Tool navigation was improved through the use of dynamic tabs. As standards are selected, the appropriate tab for access to the related question set is added to the display. If a standard is unselected, the tab is removed from the tool display.
* The report selection interface was improved. The online report now uses dynamic, standards‑driven functionality with drop-down selection lists. Both PDF and RTF formats are now available for the printed report. The format of the printed report was revised for improved readability.
* Both the online and printed reports for NERC and SANS Top 20 gaps were clarified to present a pass/fail oriented display. Previous versions of the tool presented the gaps in a format similar to the standards that relied on a SAL level for grading. The pass/fail approach is better aligned with the intent of the standards.
* Text display was improved in several dialog boxes and menu items.

**Corrected known issues**:

1. Under certain circumstances, the Document Library would allow deletion of a document even if it was associated with a question.
2. For questions with duplicate answers assigned to different SALs, the reports defaulted to the highest risk SAL (lowest SAL number) rather than to the least risk SAL (highest SAL number).
3. Under certain circumstances, when a component was deleted from the network diagram, it would remain checked in the left-hand question tree.
4. When completing the Node information for an added component, the Label field failed to auto‑populate with the entered Host Name if the user pressed the Enter key after typing the Host Name.

CS2SAT Version 1.0.1:

Version 1.0.1 was created to correct a few minor issues that had been identified after Version 1.0.0 was released. Also, a licensee requested a change to the text of the Advisory.

**Changes incorporated into Version 1.0.1 include**:

1. In the Advisory, the sentence

“Periodic onsite reviews and inspections must still be conducted using a holistic approach including scanning, penetration testing, facility walk-downs, and exercises.”

was changed to

“Periodic onsite reviews and inspections must still be conducted using a holistic approach including facility walk-downs, interviews, and observation and examination of facility practices. Consideration should also be given to additional steps including scanning, penetration testing, and exercises on surrogate, training, or nonproduction systems, or systems where failures, unexpected faults, or other unexpected results will not compromise production or safety.”

**Corrected known issues**:

1. Component question 3526 under EWS was missing the “?” icon.
2. In the printed report, DoD administrative question 2646 displayed the style text instructions rather than implementing them.
3. In the online report, help links were missing from the NERC standards section.
4. When first using the tool, documents could be added to the tool via the Document Library, but not via the question link.