INL/CON-07-12810
PREPRINT

CS^{2}SAT: The Control Systems Cyber Security Self-Assessment Tool

ISA Expo 2007

Kathleen A. Lee

January 2008

The INL is a
U.S. Department of Energy
National Laboratory
operated by
Battelle Energy Alliance

CS^2SAT: The Control Systems Cyber Security Self-Assessment Tool

Kathleen A. Lee

Keywords: assessments, cyber security, control systems, CS^2SAT, DHS, National Cyber Security Division, NCSD, NERC, CIP, compliance

ABSTRACT

The Department of Homeland Security National Cyber Security Division has developed the Control System Cyber Security Self-Assessment Tool (CS^2SAT) that provides users with a systematic and repeatable approach for assessing many programmatic and certain other aspects of the cyber-security posture of their industrial control system networks. The CS^2SAT was developed by cyber security experts from Department of Energy National Laboratories and with assistance from the National Institute of Standards and Technology. The CS^2SAT is a desktop software tool that guides users through a step-by-step process to collect facility-specific control system component information and then makes appropriate recommendations for improving the system's cyber-security posture. The CS^2SAT provides recommendations from a database of industry available cyber-security practices, some of which have been adapted specifically for application to industrial control system networks and components. Each recommendation is linked to a set of actions that can be applied to remediate-specific security vulnerabilities.

INTRODUCTION

At the heart of most critical infrastructure operations is an electrical network of computers and intelligent devices with miles upon miles of copper and fiber optic cables that enable local and remote communication with facility control rooms, area or regional control centers, dispatch offices, and engineering support centers. This same network of connectivity that enables the productivity driving business cases is also the crux of many of the modern-day cyber-security issues. Legacy control systems, which were not designed with cyber security as a priority, are now being connected to Internet accessible networks, exposing these systems to potential compromise and inadvertent operation.

As the awareness of this problem has grown, the U.S. Department of Homeland Security (DHS) National Cyber Security Division (NCSD) has been working on methods and tools to assist asset owners in evaluating the security posture of the control systems used to operate the nation's critical infrastructure. The main goal of this effort is to identify vulnerabilities and reduce the risk related to cyber threats by recommending solutions to mitigate those vulnerabilities. While the initial target has been those systems that are critical for delivering services essential to maintaining the safety and well-

being of the general public, operators of critical infrastructure are not the only beneficiaries of these tools and methods. These tools and methods are being made readily available to all those seeking assistance in improving the security posture of their systems. The NCSD Control Systems Security Program (CSSP), with the assistance of Department of Energy National Laboratories, has made a concerted effort in delivering solutions that can be used to make an immediate impact on control system security and address the long-term issue of building security into systems rather than bolting it on after the system is already in place.

Since 2004, the DHS NCSD CSSP has been working to provide a method and tool to assist in the evaluation of the cyber-security posture for control systems and provide recommendations to mitigate vulnerabilities. One of the products developed from this program is the Control Systems Cyber Security Self Assessment Tool (CS^2SAT). The CS^2SAT provides users with a systematic and repeatable approach for assessing many programmatic and certain other aspects of the cyber-security posture of their industrial control system networks. The CS^2SAT is a desktop software tool that guides users through a step-by-step process to collect significant facility-specific control system program, procedure, and certain other information and then provides appropriate recommendations for improving the owner's cyber security programs and certain aspects of the system's cyber-security posture. The tool draws its recommendations from a database of the best available cyber-security practices, some of which have been adapted specifically for application to industry control system networks and components. Each recommendation is linked to a set of actions that can be applied to remediate specific security vulnerabilities. The CS^2SAT provides the following services:

- A repeatable and systematic approach for assessing many programmatic and certain other aspects of the cyber-security posture of the industrial control system network, based on the components used in the system
- A comprehensive evaluation of programs and certain practices and comparison to existing industry standards and regulations
- Opportunity for dialogue on security practices within the facility, particularly with regard to industrial control system cyber security
- Identification of potential vulnerabilities in the facilities security policies and certain aspects of the industrial control system's design
- Guidelines for mitigation or resolution of identified vulnerabilities in the industrial control systems evaluated.

CS^2SAT BACKGROUND

The purpose of the CS^2SAT is to provide organizations that use industrial control systems to control a physical process with a self-assessment tool for evaluating the programmatic and certain other aspects of security of the control system. The CS^2SAT is designed as a self-contained tool and requirements repository to assist individuals performing an assessment in identifying actionable control system cyber security vulnerabilities and associated mitigations. The CS^2SAT is designed with an underlying cyber security framework based on federal codes, industry standards, and guidelines such as the following:

- National Institute of Standards and Technology (NIST) System Protection Profile, Critical Infrastructure Process Control Systems (SPP-CIPCS), Revision 1.07 (Draft)
- NIST SPP Industrial Control Systems (SPP-ICS), Revision 1.0
- Common Criteria, ISO/IEC 15408 Versions 2.1 to 3.0
- North American Electric Reliability Council (NERC) Critical Infrastructure Protection (CIP) Reliability Standards, CIP-002-1 – CIP-009-1
- NIST Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems, February, 2005
- U.S. Department of Defense (DoD) Instruction Number 8500.2, "Information Assurance (IA) Implementation," February 6, 2003.
- Industry Standards and Leading Practices

The tool provides question sets specific to individual standards (such as NERC CIP) and question sets tailored to individual components (such as a firewall) that reference multiple sources.

It is recommended that the CS^{2}SAT be used in a team effort, because the breadth and depth of questions invariably exceeds the knowledge of any one individual. Having a team also allows sharing of information and clarifying security configurations among members of the organization.

CS^{2}SAT OPERATION

The steps involved with performing a self-assessment with the CS^{2}SAT are (1) preparing for the assessment, (2) documenting the assessment information, (3) determining the Security Assurance Level, (4) drawing the network diagram, (5) answering the component-specific and standards-specific questions, and (6) generating the reports.

PREPARING FOR SELF-ASSESSMENT

There are two preliminary tasks required before performing a self-assessment: forming the subject matter team and collecting the industrial control systems network/architecture documentation and related information.

SUBJECT MATTER TEAM

The first step is to select a cross-functional assessment team consisting of four to five personnel selected from the various operational areas in the organization. Teams typically include representation from senior management, operations, information technology, industrial control systems (process control/SCADA), (this expertise is often from Maintenance and/or Engineering organizations within an organization), and security. Organizations may add additional team members depending upon the skills and/or expertise required to complete the assessment process.

SUPPORTING DOCUMENTATION AND INFORMATION

It is advisable to collect the following types of information in advance of performing an assessment with the CS^{2}SAT:

- Organizational chart that outlines responsibilities
- Annual operating and capital budgets
- Insurance policy description
- Previously performed risk assessment and/or vulnerability assessments
- Capacity, operation, management, and maintenance manual
- Risk management documentation
- Hazardous waste operations and emergency response standard
- Emergency operations plan or 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.
- Information security policies, plans, and procedures.

When the assessment team is prepared and supporting documents are gathered, the organization will be ready to begin the actual self-assessment.

DOCUMENTING ASSESSMENT INFORMATION

An assessment information form is provided in the tool to allow users to uniquely identify the self-assessment, including the assessment team members, assessment date, and industrial control system architecture evaluated. This information provides the organization reference information and a baseline for future assessments.

DETERMINING SECURITY ASSURANCE LEVEL

Implementation of cyber-security mitigations usually comes with a cost. This cost can come from the time to implement, ongoing maintenance, additional hardware, or degradation in performance. The key is to find a reasonable cost balance between acceptable risk and potential consequence. The CS^{2}SAT attempts to assist users in finding this balance by identifying a number of Security Assurance Levels (SALs), based on the possible consequences of a cyber attack on the system. Different levels of rigor for implementing mitigations should be used depending on the assurance levels. Simply put, the more potential for economic, environmental, or human damage, the more rigor should be placed on mitigating strategies.

The security-assurance analysis considers the worst reasonable consequence that could be generated by a specific threat scenario. The SAL provides an overall rating of criticality based on the user reviews of security scenarios and estimated consequences. The overall SAL is used to determine the assurance level used to mitigate the consequence.

Figure 1 shows the questionnaire used in determining the SAL rating to be used in the assessment. SAL levels range from 1 to 5, with 5 being the highest assurance level and requiring the greatest level of rigor in implementing the solution strategies.

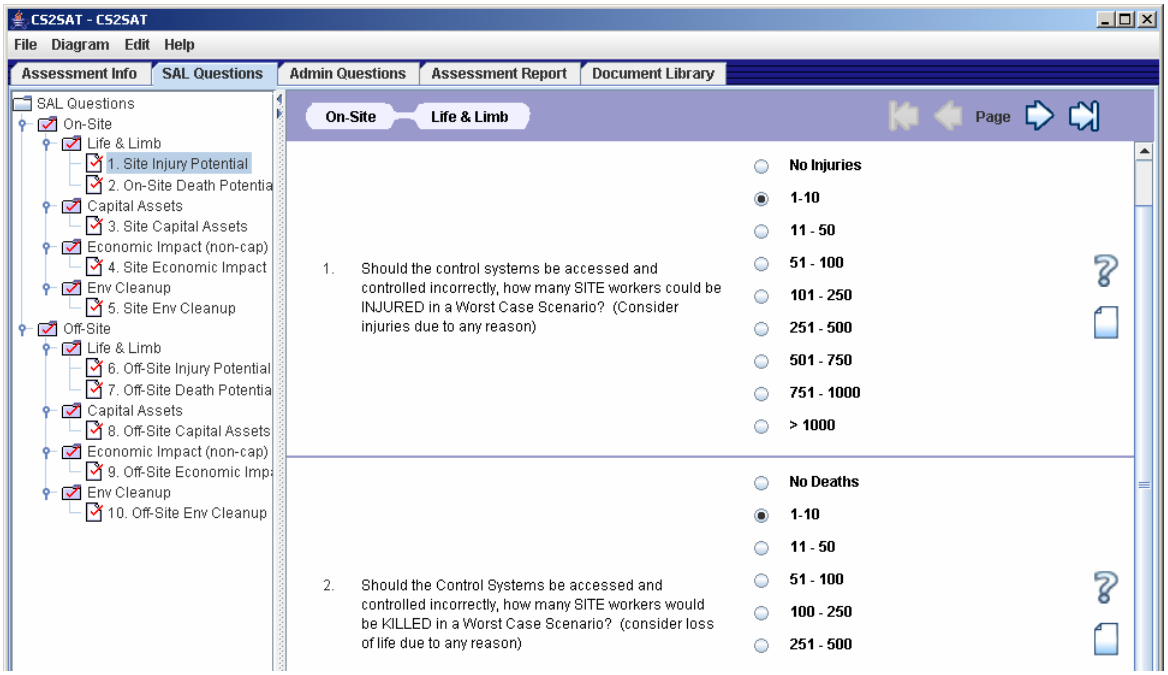

Figure 1. Security Assurance Level (SAL) questionnaire.

DRAWING NETWORK TOPOLOGY

The purpose of drawing a network topology is to build the representative network architecture to be assessed. Template diagrams are included in the tool to allow users to save time constructing their network by choosing the template that best matches their topology. The templates can be modified to reflect the actual network, or, if no template is selected, a diagram can be created from scratch using the drawing tool. The diagram, whether created from a template or from scratch, is automatically incorporated into the assessment. A sample network diagram is shown in Figure 2.

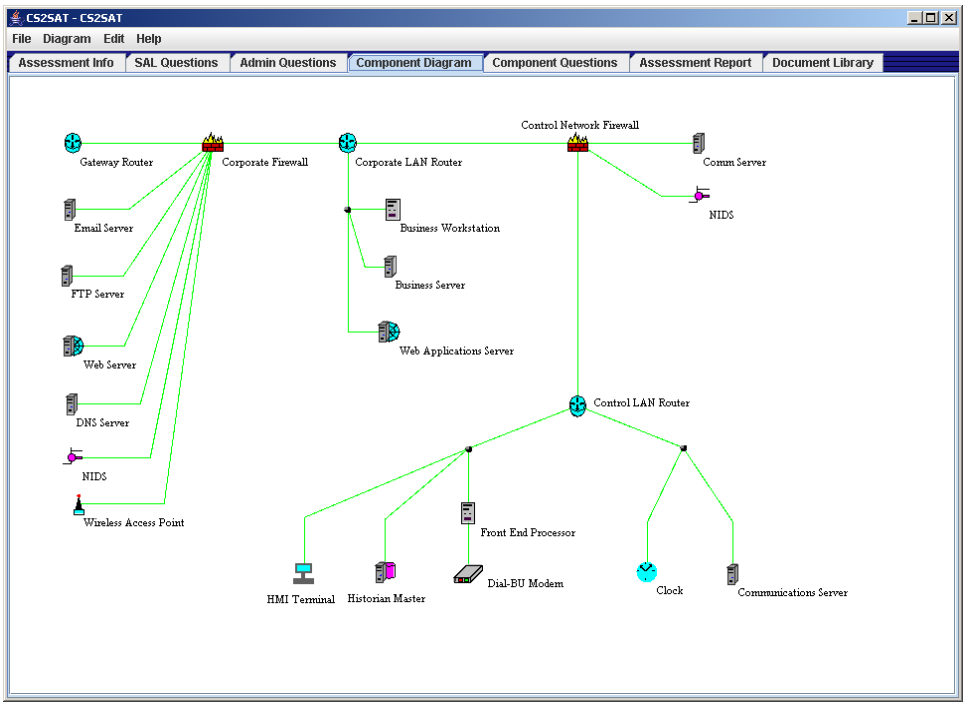

Figure 2. Network diagram.

ANSWERING QUESTIONS

A list of questions is generated specifically for the components in the network diagram. In addition to the component-level questions, system or administrative-level question sets are provided that are specific for certain standards. Figure 3 shows the four administrative-level standards currently incorporated into the tool (NERC CIP-002 through CIP-009, NIST SP800-53, ISO/IEC 15408 v. 3.1 Assurance Requirements and DoDI 8500.2).

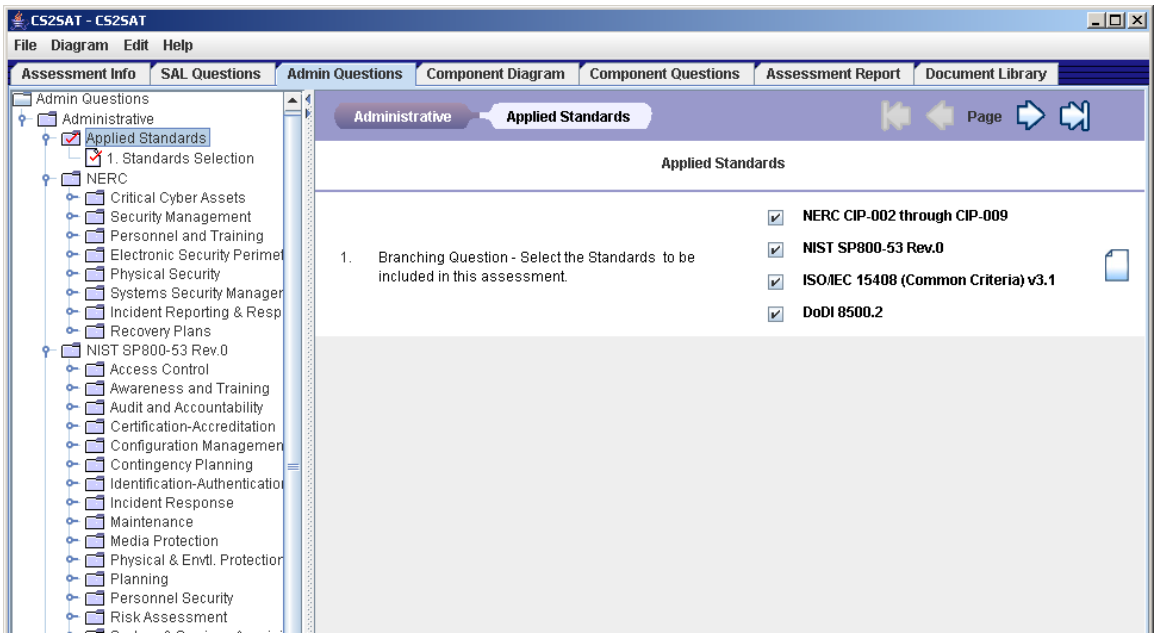

Figure 3. Administrative-level standards.

A list of components from the network diagram in Figure 2 can be seen in the left-hand window of Figure 4. The tool has generated a question-set specific for each component in the network. One such question, for the web server, is shown in Figure 4.

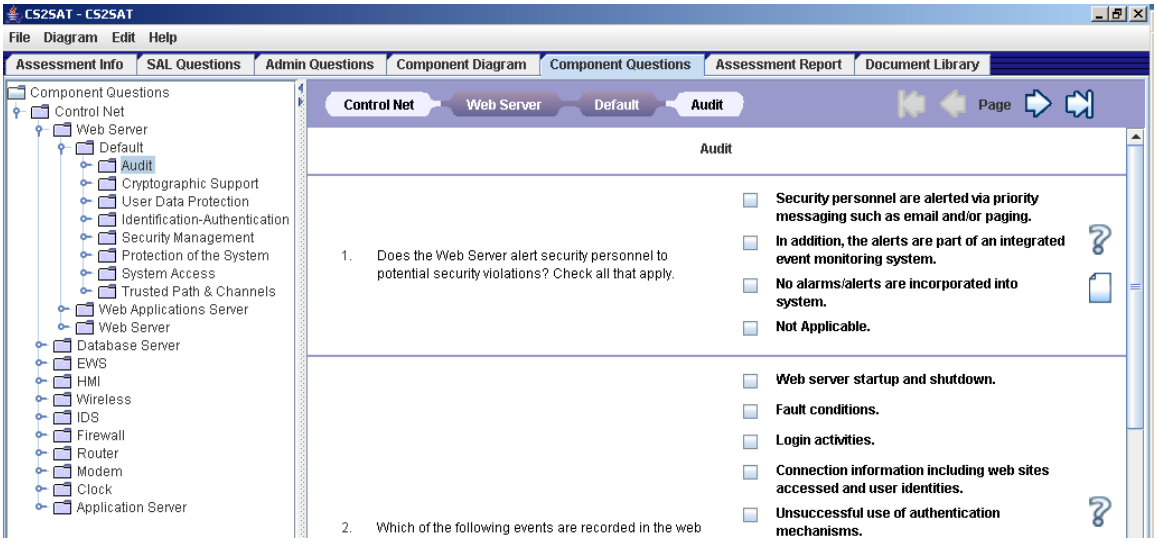

Figure 4. Component question.

Users must select the appropriate option displayed for each question. Each question is multiple choice. Some questions allow for multiple answers, in which case users are encouraged to select all answers that apply. In the case of the question shown in Figure 4, the answer that is considered “correct” depends on the SAL level determined at the start of the assessment.

Help for the question can be found by clicking on the question mark icon located to the right of each question. Selecting the paper icon (located below the question mark icon) brings up a comment box. This allows users to add information, notes, or rationale for each answer provided in the assessment. The page icon also allows for linking the question to a document in the user's Document Library. The Document Library function (see Figure 5) allows for the upload of the organization's policies and procedures. These documents can be linked to the appropriate requirement in the tool, creating a document repository for the organization's records.

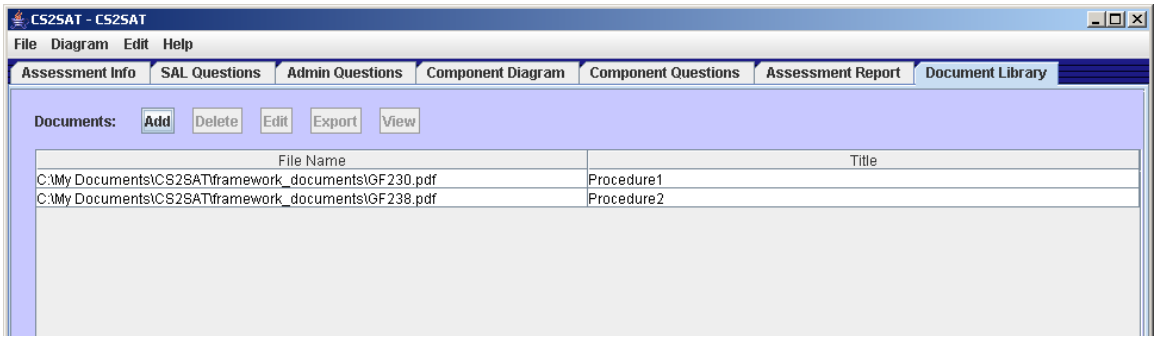

Figure 5. Document library.

GENERATING REPORTS

The CS^{2}SAT generates both online and hardcopy reports. Before generating reports, the SAL level must be entered, as shown in Figure 6. The reports are then tailored specifically for the selected SAL. The Mission Assurance Category and Confidentiality levels, shown in Figure 6, are used only for the DoD reports.

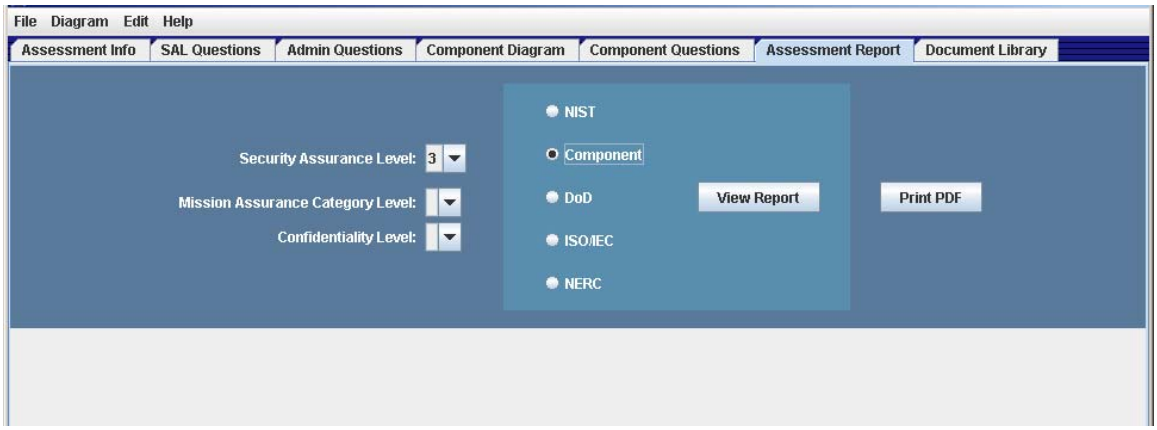

Figure 6. Report generation.

An online report is available for each of the administrative standards and for the component questionnaire, and is generated by clicking the *View Report* button. Figure 6 shows the component report selected. This report displays a listing of all the components assessed based on the component diagram that did not meet the required level of rigor specified by the established SAL.

ONLINE REPORT

A partial online report for the component questionnaire is shown in Figure 7. In the SAL column, the green highlight represents the minimum responses needed to meet the selected SAL. The red highlight indicates the SAL currently supported by the control system (as determined by the user's response). In the Required Answer(s) column, yellow highlight represents the answer provided to the question. Solution documents are provided under *Help Documents* to assist in meeting the requirement.

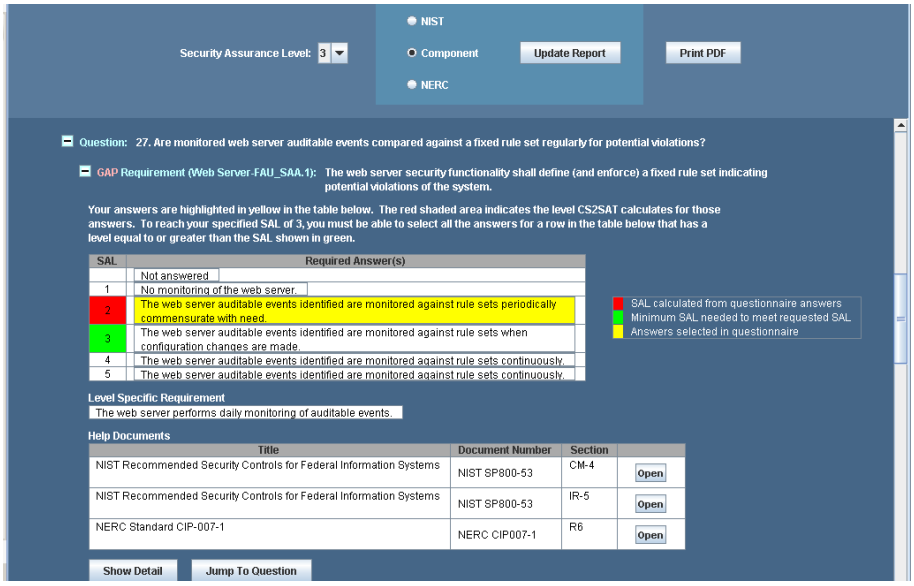

Figure 7. Online report.

HARDCOPY REPORTS

When selecting the *Print PDF* button (see Figure 6), a pop-up provides the opportunity to select from several different reports that can be generated (see Figure 8). A full assessment report can be lengthy; therefore, the tool allows smaller, targeted reports to be generated. A brief discussion of the report options follows.

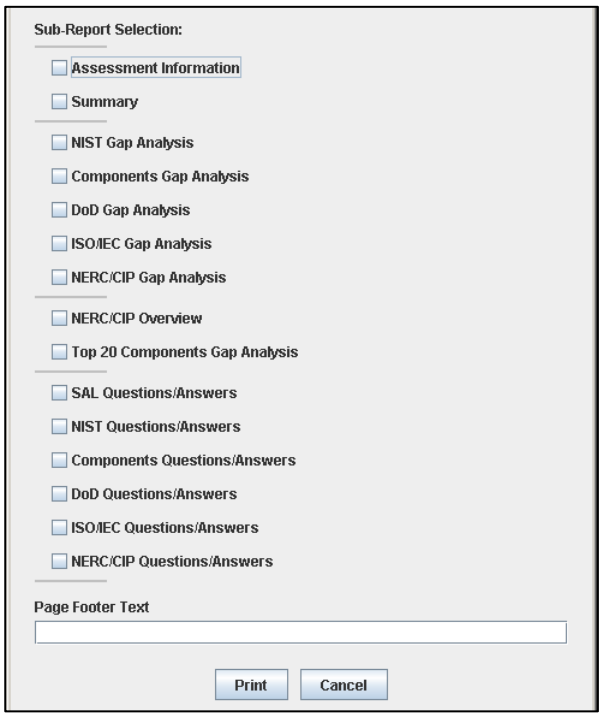

Figure 8. Report selections.

Assessment Information: This report includes information entered at the beginning of the assessment.

Summary: This report includes a series of graphical bar and pie charts that display the responses to the assessment questions (see Figures 9 and 10). In the pie charts, the green-highlighted section represents responses that met or exceeded the defined/selected SAL. Yellow, orange, and red segments represent responses that were 1, 2, 3, or more levels from the selected security level, respectively. The blue segment represents non-responses or unknown answers to the questions. These pie charts provide a quick snapshot of the security posture and an overview of how well the respondents understood the industrial control system network (as indicated by the blue segments). These pie charts are generated and arranged for (1) overall compliance representing the entire question set for all components, (2) administrative or system-level compliance, and (3) compliance for each component. The purpose of the charts is to help users to quickly identify the components on which to focus. Bar charts provide summary information for each standard in the administrative questionnaire. Figure 10 shows percentage compliance for each subject area in the NERC CIP report. Similar subject area bar charts are available for the other administrative standards.

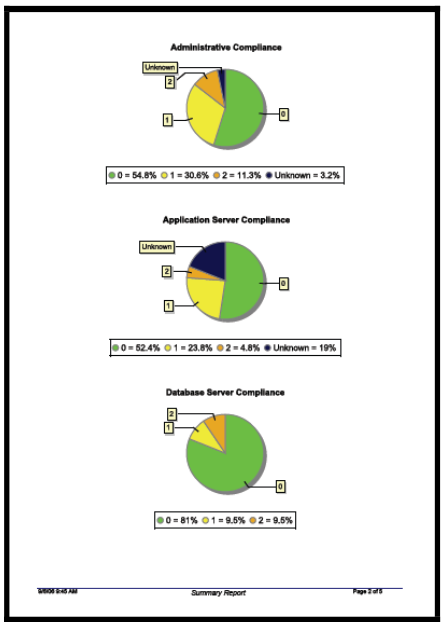

Figure 9. Summary pie chart report.

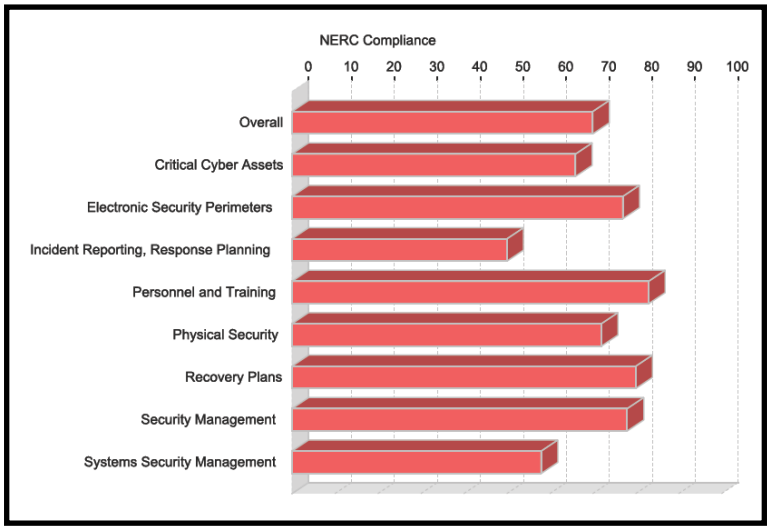

Figure 10. Summary bar chart report.

Gap Analysis: The information in this report is identical to the information provided in the online report, with the exception that supporting documentation is not given.

NERC CIP Overview: This report provides information related to the compliance to each requirement of the NERC CIP standard.

Top 20 Components Gap Analysis: This report lists the top 20 component deficiencies, which are prioritized by weighting the component's criticality in the industrial control system network, criticality of the requirement, and level of deficiency from the target based on the SAL. For example, a high

critical component with a high critical requirement that was severely deficient will be prioritized higher than non-critical component/requirement(s) that were only slightly deficient.

Questions/Answers: This is the answer key for all user responses and a summary of the SAL analysis, which is how users responded to each question, including a color-coded indication of whether the requirement was met.

SUMMARY AND RECOMMENDATIONS

The CS^{2}SAT can be an integral tool in identifying vulnerabilities in control systems operating critical infrastructure and providing actionable advice to assist in making the systems more resilient to cyber attacks. In using the CS^{2}SAT, a number of recommendations are provided. The difficult part is evaluating and implementing the solutions. The CS^{2}SAT's built-in algorithm prioritizes recommendations based on the criticality of the component in the system, importance of the requirement, and the size of gap in meeting the requirement. These three factors form the basis for identifying which recommendations are provided to the user first. However, these prioritized results still need to be evaluated for applicability and further reviewed for inclusion into an action plan.

Developing an action plan can be fairly straightforward if simple steps are taken to organize the results gathered from an assessment. First, the results can be categorized into three areas: people (behaviors), processes (policies and procedures), and technology (hardware and software). By organizing results into these groups, the task of evaluating the results becomes much easier because the information is sorted into meaningful groups with similar actionable recommendations. Each one of these groups can be further subdivided into smaller sections to add granularity in developing an action plan.

Using the CS^{2}SAT is just one step in evaluating a control system. The depth of information needed to complete the assessment is significant, and, in some instances, further inspection in the field is required to answer questions. Evaluating how well the control system is understood is achieved by identifying areas where questions could not be answered due to lack of information or simple uncertainty. The executive pie-chart summary is the quickest way to identify the areas of uncertainty and the apparent level of security implemented on the system.

The reporting function of the tool provides a quick glimpse for identifying areas of security weaknesses where answers to the question fall outside the SAL defined for the facility. The further away from the SAL, the more work is required to implement security practices to return to the SAL security baseline. The CS^{2}SAT will also identify areas where facility/operations staff do not have a clear understanding of the control system environment. These are identified by the "unknown" responses identified in the reports.

It is important to keep in mind that the CS^{2}SAT is only one component in developing an overall cyber security plan and should be complemented with a robust cyber security program within the organization. The CS^{2}SAT is not intended to be used as a substitute for in-depth analysis of control system vulnerabilities as performed by trained professionals. Periodic on-site reviews and inspections

must still be conducted using a holistic approach that includes scanning, penetration testing, facility walk-downs, and exercises.