CYBER SECURITY EVALUATION TOOL FACT SHEET FOR PUBLIC SAFETY

INTRODUCTION TO THE CYBER SECURITY EVALUATION TOOL AND MODULES

The Cyber Security Evaluation Tool (CSET®) is a free stand-alone desktop application that systematically guides asset owners and operators through evaluating operational and information technology. The Department of Homeland (DHS) Cybersecurity and Infrastructure Security Agency (CISA) offers the CSET® download at no cost. The benefits of CSET® include the:

- Creation of infrastructure security assessments through systematic, disciplined, and repeatable methods,
- Generation of baseline reports that can help determine trends by comparing multiple assessments,
- Customization of System Security Plans based upon assessment results that allow organizations to qualify their cybersecurity posture; and
- Construction of network diagrams that users can prepare from scratch or through a pre-built template diagram
- Support data export and import feature via JSON
- Create custom assessments via the Module Builder feature
- New Cyber Performance Goal Assessment that is designed to help Critical infrastructure partners

Within CSET®, there is a specific module, the Land Mobile Radio (LMR) Rapid Assessment module, designed to assist public safety LMR system owners in assessing key aspects of an LMR system's cybersecurity status. This module is based on a subset of The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, "Security and Privacy Controls for Information Systems and Organizations" controls. The module guides LMR system owners/operators through control questions so that an LMR system owner/operator can gain insights into their LMR system's cybersecurity status and identify improvement measures.[1]

CSET® HELPS IDENTIFY CYBERSECURITY GAPS

CSET® provides solutions, recommendations, and best practices to remedy identified cybersecurity gaps in an organization's network. The Tool can also provide focused solution assistance, such as mitigation techniques for identified vulnerabilities. In conjunction with the Tool, CISA offers and supplies broader capabilities and additional solution assistance support, including:

Interagency Security Committee Compliance Assistance

Cyber Incident Response Assistance

System Security Plans

[1] The CISA Protected Critical Infrastructure Information (PCII) Program is an information protection program to enhance information sharing between the private sector and government. The PCII program allows information to be shared with government agencies with the confidence that the government will not expose sensitive or proprietary data to public disclosure. Under this program, LMR owners and managers can share information about their networks and systems with the assurance that it will not become public record.

CSET® currently derives its requirements from a comprehensive series of industry standards and recognized best practices. The Tool helps to identify a variety of vulnerabilities and can suggest enhancements in the areas of:


Boundary Protection


Least Functionality


Identification and Authentication


Physical Access Control


Audit Review, Analysis, and Reporting


Authenticator Management


Least Privilege


Allocation of Resources


Remote Access


Security Awareness Training

After completing the evaluation, the organization will receive reports that present the assessment results in both summarized and detailed manners. In addition, the organization will be able to manipulate and filter content to analyze findings with varying degrees of granularity and better identify cybersecurity gaps.

CSET® PROCESS

1. ORGANIZE THE TEAM

There are tremendous advantages to assembling the team and reviewing the questions together. Every effort should be made to meet as a group and facilitate discussion.

2. DOWNLOAD CSET®

Organizations need to create a CSET® account by visiting the CSET® homepage.

3. ADD ASSESSMENT INFORMATION

This step is background information about the assessment and the content displayed in the reports.

4. SELECT THE MODE AND STANDARDS

Choose modes: universal questions or requirements-based. Next, select one or more standards to match your organization's needs.

5. DETERMINE SECURITY LEVELS

This process depends on the selected standard(s) and may include additional questions/ questionnaires. The Tool weighs the question responses based on the chosen security level.

6. ANSWER QUESTIONS

The team reviews and completes answering each question.

7. ANALYZE RESULTS

The Tool dynamically creates detailed charts based on the requirements and the selected security levels that can be used to understand strengths, weaknesses, and areas for improvement.

8. INCORPORATE RESULTS INTO NEW SOLUTIONS

New solutions and best practices can be constructed to address issues discovered during the assessment.

LAND MOBILE RADIO RAPID ASSESSMENT MODULE USING CSET®

The LMR Rapid Assessment module consists of a tailored set of NIST SP 800-53 controls covering 17 control families that apply to an LMR system. LMR system owners/operators are guided through questions specifically tailored to LMR system

configurations and use. The LMR Rapid Assessment module can be performed either as a self-assessment or as a CISA-facilitated assessment using Integrated Operations Division (IOD) Cyber Security Advisors (CSA) and/or Emergency Communication Coordinators (ECC).

The LMR Rapid Assessment module also provides detailed reports that managers can use to identify areas of concern using recognized government and industry standards. The assessment information supports the development of a system cybersecurity plan, which the public safety communications community identified as a gap

CISA recommends including LMR systems engineers, configuration managers, operations managers, network specialists, IT security officers, risk analysts or insurance specialists, and representatives from the LMR system vendor in the assessment process. Facilitated assessments would also include CISA regional ECCs and/or CSAs. CISA continues to evaluate the module and any adjustments will be made through future CSET version responses.

ADDITIONAL INFORMATION ON CSET®

CSET® VIDEOS

This video provides a quick overview of the functionality in CSET®.

This video shows a more in-depth look at CSET® functionality. This video covers beginning an assessment, creating a network diagram, answering questions, and viewing results

- For the latest web application: Download App (inl.gov) For older desktop versions: github.com/cisagov/CSET®
- To learn more about CSET®, please visit cisa.gov/cyber-resource-hub
- For any more questions, please email: CSD_VM_Methodology@cisa.dhs.gov