



NCCIC/ICS-CERT Assessment FAQs

Question	Answer
Assessment Offerings	
<p><i>What is a CSET assessment?</i></p>	<p>The Cyber Security Evaluation Tool (CSET[®]) desktop software was developed by NCCIC’s Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) and guides users through a step-by-step process to assess their control systems and information technology network security practices against recognized industry standards. The CSET output is a prioritized list of recommendations for improving the cybersecurity posture of an organization’s enterprise and industrial control cyber systems. The tool derives the recommendations from a database of cybersecurity standards, guidelines, and practices. Each recommendation is linked to a set of actions that can be applied to enhance cybersecurity controls.</p> <p>CSET has been designed for easy installation and use on a stand-alone laptop or workstation. It incorporates a variety of available standards from organizations such as the National Institute of Standards and Technology (NIST), the North American Electric Reliability Corporation (NERC), the Transportation Security Administration (TSA), the U.S. Department of Defense (DoD), and others. When the tool user selects one or more of these standards, CSET opens up a set of questions to be answered. The answers to these questions are compared against a selected security assurance level, with an individualized report generated that shows areas for potential cybersecurity improvement. CSET provides an excellent means to perform a self-assessment of the security posture of your control system environment by:</p> <ul style="list-style-type: none"> • Contributing to your organization’s risk management and decision-making process • Raising awareness and facilitating discussion on cybersecurity within your organization • Highlighting vulnerabilities in your organization’s systems and providing recommendations on ways to address the vulnerability • Identifying areas of strength and best practices being followed by your organization • Providing a method to systematically compare and monitor improvement in your cyber systems • Providing a common industry-wide tool for assessing cyber systems. <p>Select the CSET Factsheet link for more information.</p>



Question	Answer
<i>What is a DAR assessment?</i>	<p>ICS-CERT’s Design Architecture Review (DAR) provides critical infrastructure asset owners and operators with a comprehensive technical review and cyber evaluation of the architecture and components that comprise their industrial control systems (ICS) operations.</p> <p>This 2-3 day review includes a deep-dive analysis of the operational process—focusing on the underlying ICS network architecture, integration of information technology (IT) and operational technology (OT) teams, vendor support, monitoring, cybersecurity controls, and all internal and external connections.</p> <p>The ICS-CERT assessment team works interactively with your IT and operations personnel to evaluate the current architecture and processes, with a focus on three key areas:</p> <ul style="list-style-type: none">• ICS Network Architecture• Asset Inventory• Protective and Detective Controls. <p>Select the DAR Factsheet link for more information.</p>
<i>What is a NAVV assessment?</i>	<p>ICS-CERT’s Network Architecture Verification and Validation (NAVV) is a passive analysis of network header data provided by the asset owner to ICS-CERT from traffic occurring within the ICS network. Using a combination of both open-source and commercially available tools, ICS-CERT presents a strategic visualization of the network header data and device-to-device communications that are occurring within ICS network segments.</p> <p>ICS-CERT’s assessment team works interactively with your IT and operations personnel to evaluate the captured network header data, reviewing:</p> <ul style="list-style-type: none">• Protocol hierarchy and organization of network traffic• Device-to-device communications—including identification of “top-talkers” and the devices generating the most traffic• Communications traversing (or attempting to traverse) the ICS network boundary—for verification that the perimeter protections are functioning as intended• Potentially misconfigured devices—or those exhibiting suspicious or anomalous behavior• ICS protocol analysis—including an in-depth review of function codes and control parameters that are observed within the captured traffic. <p>Select the NAVV Factsheet link for more information.</p>



Question	Answer
<i>Will you be connecting to our network (i.e., scanning, penetration testing, etc.)?</i>	All three of our assessments listed above are completely hands off; we will not connect to your networks. The only information we will have access to is the information you provide us, such as network diagrams, network header data (for the NAVV assessment), and inventory lists, which we will evaluate prior to visiting with you at your facility. These documents are necessary to schedule and successfully complete your assessment.
<i>Do you do penetration testing?</i>	No. All of our assessment work is performed as a table-top discussion. If you are interested in penetration testing, please contact the National Cybersecurity Assessment & Technical Services (NCATS) program at NCATS@hq.dhs.gov . Select the NCATS Factsheet link for more information.
Data Protection	
<i>How do you protect my data?</i>	<p>Company data is protected through the Department of Homeland Security (DHS) Protected Critical Infrastructure Information (PCII) program. The PCII program was established in response to the Critical Infrastructure Information (CII) Act of 2002. The PCII program creates a new framework for protecting certain types of information once that protection is appropriately requested by the submitter. The PCII program enables members of the private sector—for the first time—to voluntarily submit confidential information regarding the nation’s critical infrastructure to DHS with the assurance that the information will be protected from public disclosure.</p> <p>All work performed by associated national laboratories is protected through contractual agreements. These agreements protect proprietary information, allowing it to be viewed securely and only by individuals performing work related to each project.</p> <p>Information submitted through the PCII program is protected from:</p> <ul style="list-style-type: none"> • The Freedom of Information Act (FOIA) • State, tribal, and local disclosure laws • Use in regulatory actions • Use in civil litigation. <p>Select the PCII Program or PCII FAQs links for more information or email pcii-info@dhs.gov.</p>



Question	Answer
<i>How will you use my data?</i>	ICS-CERT publishes an “ICS Assessments Overview and Analysis” report each Fiscal Year, which provides an overview and summary analysis of onsite assessments conducted by ICS-CERT. The data used in these reports is completely anonymized. Select the ICS-CERT Assessments link for examples of this report.
<i>How long do you keep our data?</i>	PCII is retained and protected permanently or until it is removed at the request of the asset owner.
Scheduling an Assessment	
<i>How much does an assessment cost?</i>	Because ICS-CERT’s assessment services are based on Congressional funding, they are available as onsite facilitated assessments for critical infrastructure asset owners and operators at no cost.
<i>How do I schedule an assessment?</i>	To schedule an assessment, email the ICS-CERT assessment team at ics-assessments@hq.dhs.gov . Once contact has been made, we will set up an “Offerings Call.” During this call, we will discuss the assessments we have to offer and determine if any of them are a good fit for your organization.
<i>What do I need to submit prior to scheduling an assessment?</i>	After the “Offerings Call,” should you choose to proceed with an assessment, you will be sent pre-assessment documents (i.e., Request for Technical Assistance, Logistics Form Request, and PCII Express Statement). After these documents have been submitted and approved by DHS Legal, we will request network diagrams and inventory lists to review and discuss prior to scheduling.
<i>How do I transmit (send) my data to DHS?</i>	Data is transmitted through the US-CERT secure portal or through secure Sharefile (for larger files).
Logistics	
<i>Who should be at the assessment?</i>	Please invite any personnel including control systems operators/engineers, IT, policy/management personnel, and subject matter experts who are familiar with your site’s control system architecture, topologies, and protocols to attend the assessment.
<i>How long do you need to complete the assessment?</i>	A CSET/DAR/NAVV assessment will take approximately 3-4 days to complete. Day 1) CSET Day 2) DAR Day 3) DAR/NAVV Day 4) a.m. Closeout



Question	Answer
<i>What kind of meeting space should I secure for the assessment?</i>	Please ensure that a meeting room is reserved with a projector. We recommend a round table or U-shaped table setup in the room in order to better facilitate questions and discussion.
Final Report	
<i>What is the deliverable?</i>	Upon completion of the assessment process, ICS-CERT will compile an in-depth report for the asset owner, including a prioritized analysis of key discoveries and practical mitigations for enhancing the organization’s cybersecurity posture.
<i>Who will receive the final report?</i>	The final report is sent to the POC through the US-CERT secure portal. The POC may share as they deem appropriate.
<i>How long will the report take to complete?</i>	Approximately 6-8 weeks after the completion of the assessment.
Feedback Mechanisms	
<i>How can I provide feedback after the completion of an assessment?</i>	<p>ICS-CERT uses a two-phased approach to capture post-assessment feedback, including 30-day and 180-day questionnaires, to gather information on areas of improvement for the assessments, as well as the value of recommendations provided and the asset owner’s cybersecurity posture improvement after the completion of the assessment.</p> <p>The 30-day feedback survey is typically completed during the onsite engagement. The purpose is to determine how the asset owner will use the results of the assessment.</p> <p>The 180-day feedback questionnaire takes place via conference call approximately 6 months after the delivery of the final report. The purpose of this call is to discuss the discoveries noted in the final report, the status of any mitigations you have implemented or plan to implement, and the path forward.</p>
Other	
<i>Where can I learn more about ICS-CERT’s other services and offerings?</i>	ICS-CERT offers a number of free services and products to help secure control systems. For more information, please visit our website at https://ics-cert.us-cert.gov .