4910-22-P

DEPARTMENT OF TRANSPORTATION

Federal Highway Administration

[FHWA Docket No. FHWA–2024–0005]

FHWA Adoption of Cyber Security Evaluation Tool

AGENCY: Federal Highway Administration (FHWA), U.S. Department of Transportation (DOT).

ACTION: Notice; request for comments.

SUMMARY: Following coordination with the U.S. Department of Homeland Security, FHWA announces its proposal to adopt the Cyber Security Evaluation Tool (CSET) as a voluntary tool transportation authorities can use to assist in identifying, detecting, protecting against, responding to, and recovering from cyber incidents. The FHWA requests comments on its proposal.

DATES: Comments must be received on or before [INSERT DATE 45 DAYS AFTER DATE OF PUBLICATION IN THE **FEDERAL REGISTER**]. Late comments will be considered to the extent practicable.

ADDRESSES: All comments should include the docket number that appears in the heading of this document and may be submitted in any of the following ways:

- *Electronically through the Federal eRulemaking Portal:* www.regulations.gov. This Website allows the public to enter comments on any *Federal Register* notice issued by any agency. Follow the online instructions for submitting comments.
- *Mail:* U.S. Department of Transportation, Docket Operations, M-30, West Building Ground Floor, Room W12-140, 1200 New Jersey Avenue, SE., Washington, DC 20590.
- *Hand Delivery:* U.S. Department of Transportation, Docket Operations, West Building Ground Floor, Room W12-140, 1200 New Jersey Avenue, SE.,

Washington, DC 20590 between 9 a.m. and 5 p.m., ET, Monday through Friday, except Federal holidays.

Instructions: You should identify the docket number at the beginning of your comments. Note that all comments received will be posted without change to www.regulations.gov, including any personal information provided. For more information, you may review the U.S. Department of Transportation's complete Privacy Act Statement published in the Federal Register on April 11, 2000 (65 FR 19477).

FOR FURTHER INFORMATION CONTACT: For questions about this notice, please contact Mr. Jason Carnes, FHWA Transportation Security Coordinator (202) 366-5280, or via email at Jason.Carnes@dot.gov, Federal Highway Administration, 1200 New Jersey Avenue, SE., Washington, DC 20590. Office hours are from 8 a.m. to 4:30 p.m., ET, Monday through Friday, except Federal holidays.

SUPPLEMENTARY INFORMATION:

Electronic Access

This document may be viewed online under the docket number noted above through the Federal eRulemaking portal at: www.regulations.gov. Electronic submission and retrieval help and guidelines are available on the Website. Please follow the online instructions.

An electronic copy of this document may also be downloaded from the Office of the Federal Register's Website at: www.FederalRegister.gov and the U.S. Government Publishing Office's Website at: www.GovInfo.gov.

All comments received before the close of business on the comment closing date indicated above will be considered and will be available for examination in the docket at the above address. Comments received after the comment closing date will be filed in the docket and will be considered to the extent practicable. In addition to late comments, FHWA will also continue to file relevant information in the docket as it becomes

available after the comment period closing date and interested persons should continue to examine the docket for new material.

Background

Pursuant to section 11510(b) of the Bipartisan Infrastructure Law (BIL), enacted as the Infrastructure Investment and Jobs Act (Pub. L. 117-58), FHWA is required to develop a tool to assist transportation authorities in identifying, detecting, protecting against, responding to, and recovering from cyber incidents. Safety is the top priority of DOT and FHWA. The FHWA routinely works closely and collaboratively with Federal and State agencies whose primary missions revolve around securing critical transportation infrastructure. The FHWA provides subject matter expertise to those agencies in identifying potential physical and cybersecurity threats and appropriate mitigation efforts. When presented with physical or cybersecurity questions, concerns or incidents from State, local, Tribal, and Territorial transportation authorities, or other stakeholders, FHWA routinely assists in connecting these entities to security-focused government agencies, including the Transportation Security Administration (TSA), Cybersecurity and Infrastructure Security Agency (CISA), and Federal Bureau of Investigation (FBI).

In accordance with BIL, section 11510(b), FHWA is proposing to adopt CISA's CSET as a voluntary tool that transportation authorities can use to assist in identifying, detecting, protecting against, responding to, and recovering from cyber incidents. The CISA's cybersecurity mission is to defend and secure cyberspace by leading national efforts to drive national cyber defense, resilience of national critical functions, and a robust technology ecosystem. The FHWA therefore thinks it is appropriate to leverage CISA's expertise instead of attempting to create a separate and potentially duplicative tool. The CSET, developed by CISA, is a comprehensive software tool designed to assist organizations in assessing their cybersecurity posture and developing structured

improvement programs. The CSET helps organizations evaluate their cybersecurity practices, identify vulnerabilities, and prioritize mitigation efforts by providing a systematic approach to assess cybersecurity controls and processes. It offers a range of modules and questionnaires tailored to different critical infrastructure sectors, making it a valuable resource for organizations seeking to enhance their cybersecurity resilience through a well-structured assessment and development program. The CSET is available to the public for download at https://www.cisa.gov/downloading-and-installing-cset.

In proposing to adopt this voluntary tool to assist transportation authorities regarding cyber incidents, FHWA has coordinated with CISA and TSA, and consulted with appropriate stakeholders on the viability and usefulness of the tool. The feedback received confirmed that State agencies currently depend on a diverse array of cybersecurity tools sourced from multiple stakeholders, encompassing both public and private entities. Among these tools, several States choose to employ the CSET, while others customize alternative cybersecurity solutions to align with their distinct mission requirements. In addition, many State departments of transportation employ a variety of tools encompassing intrusion detection systems, vulnerability scanners, and encryption technologies to fortify their cyber defense postures, reflecting the complexity and diversity of their security strategies. The FHWA will continue to partner with other Federal Agencies that have the primary statutory mission to develop security-related cybersecurity tools to ensure highway-related equities are considered and incorporated appropriately.

Request for Comments

The FHWA requests comments regarding the Agency's proposal to adopt CISA's CSET as a voluntary tool transportation authorities can use to provide assistance regarding cyber incidents.

Further Proceedings

After considering public comments in response to this notice, FHWA will publish a notice in the *Federal Register* adopting a final cybersecurity tool.

Authority: Sec. 11510, Pub. L. 117-58, 135 Stat. 592.

Shailen P. Bhatt,
Administrator,
Federal Highway Administration.

[FR Doc. 2024-04616 Filed: 3/4/2024 8:45 am; Publication Date: 3/5/2024]