MARK E. GREEN, MD, TENNESSEE
CHAIRMAN

BENNIE G. THOMPSON, MISSISSIPPI
RANKING MEMBER

One Hundred Eighteenth Congress
Committee on Homeland Security
U.S. House of Representatives
Washington, DC 20515

March 22, 2023

The Honorable Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency
Department of Homeland Security
245 Murray Lane
Washington, DC 20528

Dear Director Easterly:

I write to inquire about the Cybersecurity and Infrastructure Security Agency's (CISA) long-term vision for the Industrial Control Systems Cybersecurity Training Initiative. Congress authorized this vital program in the *James M. Inhofe National Defense Authorization Act for Fiscal Year 2023*[1] based on a provision I authored.[2] Understanding how CISA plans to utilize this authority and build on its existing efforts will help Congress better support the program going forward.

We know that our most formidable adversaries are focused on developing their ability to launch cyber attacks on industrial control systems (ICS). The recently-released *Annual Threat Assessment of the U.S Intelligence Community* explained that "China almost certainly is capable of launching cyber attacks that could disrupt critical infrastructure services within the United States, including against oil and gas pipelines, and rail systems."[3] Additionally, "Russia is particularly focused on improving its ability to target critical infrastructure, including underwater cables and industrial control systems, in the United States as well as in allied and partner countries."[4]

The Intelligence Community's conclusions underscore the importance of strengthening the ICS cybersecurity skills of our Nation's workforce. As Congress begins its work on the Fiscal Year 2024 Department of Homeland Security appropriations bill, it is important to ensure that this vital training program is adequately resourced, so we can continue to strengthen our capacity to defend industrial control systems (ICS) from cyber threats.

---

[1] James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, Pub. L. No. 117-263, § 7122 (Dec. 23, 2022) (codified at 6 U.S.C. 2220E).
[2] Industrial Control Systems Cybersecurity Training Act, H.R. 7777, 117th Cong. (2022).
[3] Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community*, 10 (Feb. 6, 2023), https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf.
[4] *Id*. at 15

In order to gain a better understanding of the resources CISA has dedicated to ICS training and how CISA will build on those efforts, please respond to the following questions by April 21, 2023:

1. How much funding and staff have been allocated to ICS training in Fiscal Year 2023? Under the President's Budget Request for Fiscal Year 2024, how much funding and staff at CISA would be available for ICS training?

2. How many individuals and private sector partners participated in the ICS training program in Fiscal Year 2022? What is the expected level of participation in Fiscal Year 2023?

3. If Congress provided additional resources to CISA for ICS training in Fiscal Year 2024, how would CISA plan to expand access or participation in ICS training?

4. As required by Section 2220E(b), how is CISA consulting with the private sector and sector risk management agencies to ensure that the program's resources and curriculum meet industry needs?

5. How does CISA utilize threat intelligence to inform course offerings?

Last year's enactment of the *Industrial Control Systems Cybersecurity Training Act* demonstrates that ICS workforce training is a bipartisan, bicameral priority. I look forward to receiving your response and partnering with you to continue strengthening our cyber workforce.

Sincerely,

Eric Swalwell
Ranking Member
Subcommittee on Cybersecurity and Infrastructure Protection
Committee on Homeland Security

CC: The Hon. Andrew Garbarino
Chairman
Subcommittee on Cybersecurity and Infrastructure Protection
Committee on Homeland Security