Testimony

Eric Goldstein

Executive Assistant Director for Cybersecurity

Cybersecurity and Infrastructure Security Agency

U.S. Department of Homeland Security

FOR A HEARING

BEFORE THE UNITED STATES HOUSE OF REPRESENTATIVES

Committee on Homeland Security

Subcommittee on Cybersecurity, Infrastructure Protection & Innovation

Industrial Control Systems

September 15, 2022

Washington, D.C.

Chairwoman Clarke, Ranking Member Garbarino, and members of the Subcommittee, thank you for your invitation to testify today on behalf of the Cybersecurity and Infrastructure Security Agency. I appreciate the opportunity to highlight how CISA supports our Nation's industrial control systems (ICS) and operational technology (OT) communities against cyber threats that have the potential of impacting National Critical Functions and the provision of essential services to the American people.

As reflected in President Biden's National Security Memorandum (NSM) – 5, "Improving Cybersecurity for Critical Infrastructure Control Systems," securing ICS and OT assets is a top priority of the Biden-Harris Administration, and CISA is privileged to serve in a central role in implementing this directive, alongside our Federal and industry partners. NSM-5 directed an unprecedented focus on ICS cybersecurity across the U.S. government through a series of "sprints" focused on the electricity, pipeline, and water sectors and through the development of baseline cybersecurity performance goals.

Our Nation's ICS and OT community is a complex ecosystem comprised of device manufacturers, integrators, owners and operators of critical infrastructure, and security providers. CISA serves as a trusted partner within the ICS and OT ecosystem to provide information, guidance, and capabilities that enable faster and more scalable reduction of risks facing ICS and OT assets. Our goal is to meet the unique requirements of the ICS and OT community by continuously evaluating and improving our capabilities to support the areas of greatest need, recognizing that many ICS and OT environments require approaches and solutions that differ from traditional Information Technology environments.

Operational Collaboration

Over the past decade, we learned that traditional methods of public-private partnership characterized by intermittent, unidirectional information sharing did not scale to meet the pace of the adversary or the velocity of technological change. With the support of Congress, we shifted the paradigm towards continuous collaboration to empower synchronized cybersecurity planning, cyber defense, and response. The Joint Cyber Defense Collaborative (JCDC) brings together critical partners in government and the private sector to engage in persistent collaboration and joint cyber defense planning.

In April 2022, we expanded the JCDC to focus on ICS security and brought in new partners to help lead this important work. Through the creation of focused collaboration channels, the JCDC-ICS is positioned to quickly share, analyze, and enrich information about threats and vulnerabilities affecting ICS assets. Additionally, the JCDC-ICS initiative catalyzed a new planning effort intended to expedite collaboration across the ICS ecosystem, bringing together government, critical infrastructure operators, ICS vendors, and ICS security providers with unprecedented cohesion and scale. As we

continue to bring on new partners, CISA will mature the JCDC's structure and operational approaches to maximize value for the ICS community.

Serving as an Authoritative Source of Trusted Information

As a core part of our mission to advance security of the ICS and OT communities, CISA collaboratively develops trusted information to help organizations more effectively mitigate vulnerabilities. This information generally takes two forms.

First, we develop Cybersecurity Advisories with inter-agency and international partners on urgent threats and risks, such as the joint product with the National Security Agency (NSA) and Federal Bureau of Investigation (FBI) from April 13, 2022, on APT cyber tools targeting ICS/SCADA devices; our joint product with the Department of Energy (DOE) on March 29, 2022, regarding targeting uninterruptable power supplies; and our March 24, 2022, joint product with FBI and DOE on threats from Russian state-sponsored cyber actors targeting the energy sector. These products, many of which benefitted from input from private sector partners, are intended to turn raw intelligence into actionable guidance information with increased speed for organizations across the country.

Second, CISA's ICS Vulnerability Response and Disclosure program regularly publishes ICS Advisories to share information about impactful vulnerabilities. The program serves as a trusted partner with cybersecurity researchers and product vendors to effectively identify, enable mitigation, and publicly disclose vulnerabilities impacting control systems and operational technology. CISA coordinated the timely disclosure of thousands of vulnerabilities and their associated mitigations, which otherwise would affect systems and hardware supporting critical functions such as the electric grid, hospitals, building automation systems, defense systems, data centers, and other crucial systems. In 2022, CISA already has published over 300 such Advisories representing thousands of vulnerabilities in a variety of ICS/OT products. These vulnerabilities impact products used across a wide variety of sectors, including Energy, Critical Manufacturing, Water and Wastewater Systems, Food and Agriculture, and Chemical. We work closely with stakeholders across government and industry to identify the most impactful ways to disseminate vulnerability information, including through machine-readable data that can be ingested and actioned through automation and by providing guidance that enables prioritization of the most significant risks. CISA will soon begin producing machine-readable ICS Advisories in the Common Security Advisory Framework (CSAF) format, which will enable automated and timely exchange of vulnerability advisory information in an interoperable manner, and we urge all vendors of ICS and OT products to adopt this approach.

Enabling Operational Visibility

A prerequisite for optimized operational collaboration and provision of timely, actionable guidance is visibility into the targeting of ICS and OT systems. We must know how malicious actors are attempting to compromise systems, where they are succeeding, and which security measures are most effective in stopping them. To gain visibility into the breadth of malicious activity targeting American networks, we work with our JCDC partners to build an ecosystem of continuous collaboration where traffic or an incident seen by one partner can be rapidly shared across both private and public sector entities for analysis, enrichment, and correlation. To gain deeper visibility into particular sectors, we are partnering with a small number of ICS security companies to give our analysts the ability to determine whether a given threat has been seen before, while preserving anonymity of the security companies' customers.

Finally, for select critical infrastructure entities, we provide access to our CyberSentry program. CyberSentry is a CISA-managed threat detection and monitoring program that allows our analysts to directly detect attempts to compromise critical ICS networks. Through a strategic and narrow deployment, CyberSentry leverages sensitive data to provide enhanced visibility that can be used by CISA and our partners to better defend critical infrastructure networks. CyberSentry is not a replacement for a company's own ICS cybersecurity program or security providers; rather, this program provides an additive layer of visibility where the nation needs it most. We continue to encourage all organizations to adopt commercial ICS monitoring solutions by publishing guidance that provides a list of criteria organizations should consider when evaluating a commercial ICS monitoring solution. We are grateful to Congress for authorizing the CyberSentry program, and we look forward to expanding it to additional partners in the months to come.

Enabling Prioritized Investment

A key pillar of President Biden's NSM-5 directed CISA and NIST to develop cybersecurity performance goals for critical infrastructure, which "should serve as clear guidance to owners and operators about cybersecurity practices and postures that the American people can trust and should expect for such essential services." Referred to as the Common Baseline, it aims to identify a set of practices that critical infrastructure owners and operators should employ to protect systems supporting National Critical Functions and reduce risks to national security, economic security, and public health and safety. This Common Baseline represents a combination of best practices for IT and OT owners and sets forth a prioritized list of security controls. These practices are also intended to be a benchmark for critical infrastructure operators to measure and improve their cybersecurity maturity.

Unlike other control frameworks, the Common Baseline considers not only the practices that address risk to individual entities, but also the aggregate risk to the nation. Rather than a comprehensive catalog, the Common Baseline captures a core set of high-impact controls and practices with known risk-reduction value that are broadly applicable across sectors. Organizations can use the Common Baseline to prioritize the security controls which work most effectively to reduce risk in their environments. This prioritization can help determine how to most prudently allocate investments towards specific security practices.

The Common Baseline is voluntary by design, and the draft goals were developed through a highly collaborative process. CISA received over 2,000 comments across two separate rounds of review, which included multiple workshops with critical infrastructure partners, ICS and OT experts, and the general public. Importantly, the Common Baseline is designed to be utilized in conjunction with and in support of the NIST Cybersecurity Framework (CSF), which is the de facto standard for all organizations to build and evaluate their cybersecurity programs. The Common Baseline extends the CSF by identifying the most impactful controls across both IT and OT systems and describes both the scope and measurements for those controls so that it is easier for asset owners to implement and attest to their security posture. Organizations that are already using the NIST CSF or other frameworks can easily determine where they are already making progress toward achieving particular goals in the Common Baseline and where more investment may be required. We look forward to releasing the next iteration of the Common Baseline this fall, with continued collaboration across the cybersecurity community on further maturation of the baseline goals and sector-specific goals.

Conclusion

Advancing the security and resilience of industrial control systems (ICS) will continue to be a top priority for CISA and the Biden-Harris Administration. As the lead agency for civilian cybersecurity and the national coordinator for critical infrastructure security and resilience, we will continue to partner with organizations across the ICS and OT ecosystem to identify and reduce risk facing our nation's most critical systems. With the continued support of Congress, we will make measurable progress toward these essential goals.

****END****