TESTIMONY OF

Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security

BEFORE

Committee on Homeland Security
Subcommittee on Cybersecurity and Infrastructure Protection

ON

"*CISA 2025: The State of American Cybersecurity from CISA's Perspective*"

April 27, 2023
Washington, D.C.

Chairman Garbarino, Ranking Member Swalwell, and Members of the Subcommittee, thank you for the opportunity to testify regarding the priorities of the Cybersecurity and Infrastructure Security Agency (CISA) in the coming year.

In today's interconnected society, our Nation faces a wide array of serious risks from many threats, all with the potential for significant consequences that can impact our critical national functions. These functions are built as "systems of systems" with complex designs, numerous interdependencies, and inherent risks. While this structure allows for significant gains in efficiency and productivity, it also allows opportunities for nation-state actors and criminals, foreign and domestic, to undermine our national security, economic prosperity, and public health and safety, creating cascading effects across our Nation.

As the Nation's cyber defense agency, CISA is charged with leading the national effort to understand, manage, and reduce risk to the cyber and physical infrastructure Americans rely on every hour of every day. Securing our Nation's critical infrastructure is a shared responsibility requiring not just a whole-of-government, but a whole-of-Nation approach. CISA is only able to accomplish our mission by building collaborative, trusted partnerships across all levels and branches of government, the private sector, academia, and the international community. CISA's Joint Cyber Defense Collaborative (JCDC), for the first time, enables the government, the private sector, and U.S. international partners to come together to develop joint cyber defense plans and enable real-time information sharing.

As part of this mission, CISA plays two key operational roles. First, we are the operational lead for federal cybersecurity, charged with protecting and defending Federal Civilian Executive Branch (FCEB) networks (e.g., the ".gov"), in close partnership with the Office of Management and Budget, the Office of the National Cyber Director, and agency Chief Information Officers and Chief Information Security Officers. Second, we serve as the coordinator of a national effort for critical infrastructure security and resilience, working with partners across government and industry to protect and defend the nation's critical infrastructure. In both roles, CISA leads incident response to significant cyber incidents in partnership with the Federal Bureau of Investigation (FBI) and the Intelligence Community.

I am truly honored to appear before this Committee today to discuss CISA's critical mission and our exceptional workforce that works tirelessly every day to fulfill it. Since being sworn in as Director, I continue to be impressed with the talent, creativity, and enthusiasm of the dedicated CISA employees I am entrusted to lead. I have the best job in government.

CISA 2023 and 2024 Priorities

Looking forward into the coming year, CISA will remain focused on strengthening our Nation's cyber and physical defenses. We will work closely with our partners across every level of government, in the private sector, and with local communities to protect our country's networks and critical infrastructure from malicious activity and will continue to share timely and actionable information, intelligence, and guidance with our partners and the public to ensure they have the tools they need to keep our communities safe and secure and increase nationwide cybersecurity preparedness.

Overall, we continue to make critical investments in our mission-enabling activities and functions that will mature the Agency and better support the execution of our operational capabilities. CISA's Mission Support program provides enterprise leadership, management, and business administrative services that sustain day-to-day management operations for the Agency. This is essential to ensure we can hire a diverse and talented workforce and execute our missions with the technology and speed that keep us ahead of our adversaries.

CISA is also focused on the work we must do to implement the *Cyber Incident Reporting for Critical Infrastructure Act* (CIRCIA). CISA must ensure that it has the staffing, processes, and technology capabilities in place to successfully implement and utilize information provided through CIRCIA. We must engage in additional outreach efforts regarding the notice of public rulemaking and the planning efforts required to educate covered entities and CISA stakeholders on the cyber incident reporting requirements, reporting protocols, and reporting methods, as well as voluntary reporting options. In addition to the rulemaking process, CISA must ensure we can receive, manage, analyze, secure, and report on incidents reported under CIRCIA, maturing our current ability to receive and analyze incident reports, manage incidents, coordinate with and notify the interagency, and implement incident data protection functions required by CIRCIA.

Cybersecurity

The Cybersecurity Division (CSD) spearheads the national effort to ensure the defense and resilience of cyberspace. CSD will continue to build the national capacity to detect, defend against, and recover from cyberattacks. CSD will continue working with federal partners to bolster their cybersecurity and incident response postures and safeguard FCEB networks that support our Nation's essential operations. CSD will also continue our critical work partnering with the private sector and State, Local, Territorial, and Tribal (SLTT) governments to detect and mitigate cyber threats and vulnerabilities before they become incidents.

New efforts at CSD will include initiating the Joint Collaborative Environment (JCE), which will enable CSD to develop an internal analytic environment that provides more efficient analysis of mission-relevant classified and unclassified data through automation and correlation to identify previously unidentified cybersecurity risks. The JCE enables CSD to fulfill its mission and better integrate cyber threat and vulnerability data that CISA receives from our federal, SLTT, and private sector stakeholders, and rapidly work with those stakeholders to reduce associated risk. To effectively execute our role as the operational lead for federal civilian cybersecurity, CSD must maintain and advance our ability to actively detect threats targeting federal agencies and gain granular visibility into the security state of federal infrastructure. To effectuate these goals, CSD continues to mature the National Cybersecurity Protection System (NCPS) and Cyber Analytics Data System (CADS).

In the coming year, portions of the NCPS will transition to the new CADS program with intrusion detection and intrusion prevention capabilities remaining under the legacy program. CADS will provide a robust and scalable analytic environment capable of integrating mission visibility data sets, visualization tools, and advanced analytic capabilities to cyber operators. CADS tools and capabilities will facilitate the ingestion and integration of data as well as orchestrate and automate analysis that supports the rapid identification, detection, mitigation, and prevention of malicious cyber activity.

Together with the Continuous Diagnostics and Mitigation (CDM) program, these programs provide the technological foundation to secure and defend FCEB departments and agencies against advanced cyber threats. CDM enhances the overall security posture of FCEB networks by providing FCEB agencies and CISA's operators with the capability to identify, prioritize, and address cybersecurity threats and vulnerabilities, including through the deployment of Endpoint Detection and Response (EDR), cloud security capabilities, and network security controls.

CSD will continue to advance the CyberSentry program, which is a voluntary partnership with private sector critical infrastructure operators designed to detect malicious activity on the Nation's highest-risk critical infrastructure networks. CyberSentry provides best-in-class commercial technologies that allow both CSD analysts and each partner organization to rapidly detect threats that attempt to move from an organization's business network to impact industrial control systems. While CyberSentry is intended only for the most at-risk or targeted critical infrastructure entities, CSD intends to deploy capabilities to additional critical infrastructure partners to meet significant demand for the program based upon operational successes achieved to date.

Integrated Operations

The Integrated Operations Division (IOD) coordinates CISA operations at the regional level and delivers CISA capabilities and services to support stakeholders in preparing for, mitigating, responding to, and recovering from incidents that impact critical infrastructure. Additionally, IOD monitors and disseminates cyber and physical risk and threat information; provides intelligence context to support decision making; and performs Agency-designated Emergency Support Functions. IOD will continue to enable seamless and timely support to CISA stakeholders across the Nation, meeting our partners where they are in communities in every state.

Infrastructure Security

CISA's Infrastructure Security Division (ISD) leads and coordinates national programs and policies on critical infrastructure security, including conducting vulnerability assessments, facilitating exercises, and providing training and technical assistance. ISD's mission focuses on efforts such as reducing the risk of targeted violence directed at our Nation's schools, communities, houses of worship, and other public gathering locations. In addition, ISD leads programmatic efforts to secure our Nation's chemical infrastructure through implementation of the Chemical Facility Anti-Terrorism Standards (CFATS) regulation, authority for which is expiring on July 27, 2023.

Emergency Communications

CISA's Emergency Communications Division (ECD) enhances public safety communications at all levels of government across the country through training, coordination, tools, and guidance. ECD leads the development of the National Emergency Communications Plan (NECP) and 56 Statewide Communications Interoperability Plans to maximize the use of all communications capabilities—voice, video, and data—available to emergency responders and to

ensure the security of data exchange. ECD also assists local emergency responders to communicate over commercial networks during natural disasters, acts of terrorism, and other significant disruptive events. The Emergency Communications program supports nationwide sharing of best practices and lessons learned through facilitation of SAFECOM and Emergency Communications Preparedness Center governance bodies.

Stakeholder Engagement

The Stakeholder Engagement Division's (SED) activities focus on fostering collaboration, coordination, and a culture of shared responsibility for national critical infrastructure risk management with federal, SLTT, and private sector partners in the United States, as well as international partners. SED also executes CISA's roles and functions as the Sector Risk Management Agency (SRMA) for eight of the Nation's 16 critical infrastructure sectors and will lead coordination with SRMAs, the broader national voluntary critical infrastructure partnership community, and across all sectors to ensure the timely exchange of information and best practices. In partnership with the Federal Emergency Management Agency (FEMA), SED will continue implementing the State and Local Cybersecurity Grant Program, to include providing subject matter expertise and leading program evaluation efforts to ensure state and local entities can access grant resources to enhance cybersecurity resiliency and reduce cybersecurity risk.

National Risk Management Center

The National Risk Management Center (NRMC) develops analytic insights to identify and advance risk mitigation opportunities that improve national security and resiliency across critical infrastructure sectors. These analytic products support investment and operational decision making throughout the public and private sectors. The NRMC will continue two critical efforts related to SRMAs and National Critical Function (NCF) Analytics in the coming year.

First, the NRMC will continue to expand risk analysis and risk management across high priority critical infrastructure sectors. This risk analysis provides insight into cross-sectoral risk and significant sector-specific risks to support all of CISA in routinely identifying and prioritizing focused risk management opportunities to create tangible risk reduction outcomes. Second, the NRMC will continue our NCF efforts to enhance analytic capabilities, including methodology and framework development to identify and characterize critical infrastructure interdependencies within and across NCFs. This includes applied analysis to meet specific analytic requirements in the infrastructure community to enable CISA to understand consequences that extend beyond a single sector.

Conclusion

I am honored to represent my dedicated teammates at CISA who work indefatigably in support of our mission to understand, manage, and reduce risk to our cyber and physical infrastructure. The risks we face are complex, geographically dispersed, and affect a diverse array of our stakeholders, including federal civilian government agencies, private sector

companies, SLTT governments, and ultimately the American people. However, CISA stands ready to carry out these critical mission imperatives.

Before I close, I would like to take a moment to recognize the Homeland Security Committee's and this Subcommittee's strong support for CISA. For myself, and on behalf of our CISA workforce, thank you for your support. As one team unified behind our shared mission, we will continue to operate in an efficient and cost-effective manner. There is much work to be done and I look forward to working with you during the 118th Congress to continue strengthening this Agency, and by extension, the security and resilience of our Nation's networks and critical infrastructure.

Thank you for the opportunity to appear before you today, and I look forward to your questions.