COMMITTEE ON HOMELAND SECURITY

Ranking Member Bennie G. Thompson

FOR IMMEDIATE RELEASE

Hearing Statement of Cybersecurity & Infrustructure Protection Subcommittee Ranking Member Eric Swalwell (D-CA)

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

April 27, 2023

CISA is at an inflection point. Congress made CISA an operational component of DHS nearly five years ago. Since then, its budget has nearly doubled and Congress has provided it a range of new authorities – from mandatory cyber incident reporting, to persistent threat hunting on Federal networks, to CyberSentry. And CISA has ambitiously taken on new responsibilities to meet the demands of the evolving threat landscape, building trusted relationships with new stakeholders in the process.

I commend CISA for its proven ability to dynamically respond to evolving threats, ranging from election security to open source software vulnerabilities to the Shields Up campaign. It has launched promising new initiatives, including the National Risk Management Center and the Joint Cyber Defense Collaborative, aimed at maturing how the government understands systemic risk and operationalizes partnerships across agencies and with the private sector. All of these are worthy efforts. I support them, and I am committed to their success.

Today, I look forward to hearing how CISA will continue to be deliberate in the new work it takes on and the commitments it makes to its partners. As more stakeholders become aware of CISA and its capacity, they have placed more and more demands on its resources. CISA cannot be everything to everyone, and it cannot boil the ocean. Becoming the powerhouse cybersecurity and critical infrastructure defense agency CISA has the potential to be requires clear strategic direction and determined leadership. I have every confidence that Director Easterly has both, and I will be interested in learning more about her vision for CISA moving forward.

I am also interested in discussing the future of JCDC. Stakeholders applaud JCDC as an innovative, flexible tool for CISA to gather and fuse threat information, foster real-time collaboration, and push out security practices through initiatives like its 'Shields Up' campaign. Over the past year-and-a-half CISA has expanded JCDC's focus to include open source software security and protecting high-risk communities like journalistic or civil society organizations. Although these are worthwhile efforts, it is unclear what criteria JCDC is using to select which areas to focus on, which organizations to partner with (and for what reason), and how these activities are tied to the JCPO's original purpose of streamlining cyber planning and operational collaboration.

I look forward to candid conversations about defining JCDC's core functions, how to ensure JCDC partners are involved in decisions about its future, and how it can bring a more proactive posture to CISA's defensive activities. Formalizing the answers to these questions through authorization will ensure JCDC has enduring value for years to come. On a related note, I understand that CISA is in the process of revamping the National Risk Management Center, and I look forward to learning more about plans to make it CISA's analytical hub. As with JCDC, I believe NRMC would benefit from authorization and hope to work with you on that effort as you finalize the restructuring process.

Finally, it is critically important that CISA do more to secure industrial control systems (ICS) and other operational technology (OT). These systems deliver indispensable services – the water we drink, the energy that powers our home, the gas we put in our cars, the goods we manufacture, and countless others. They are also increasingly

connected to the internet, uniquely vulnerable, and require specialized expertise to secure – and we don't have nearly enough OT security professionals in the workforce today.

I appreciate CISA's support for my legislation that we passed into law last year, the Industrial Control Systems Cybersecurity Training Act, which will solidify the existence of meaningful training courses to ensure OT remains at the forefront of our security focus. As I am sure you will agree, CISA must develop that workforce now, not 5 years from now – while also doing more to understand threats to OT systems, push out its Cyber Performance Goals, and grow programs like Cyber Sentry that help to monitor OT threats.

# # #

Media contact: Adam Comis at 202-225-9978