Testimony of Robert K. Knake

Deputy National Cyber Director for Strategy and Budget & Acting Deputy National Cyber Director

United States House of Representatives

Committee on Homeland Security

Subcommittee on Cybersecurity, Infrastructure Protection, & Innovation

"Mobilizing our Cyber Defenses: Maturing Public-Private Partnerships to Secure U.S. Critical Infrastructure"

April 6, 2022

Chairwoman Clarke, Ranking Member Garbarino, distinguished members of the Subcommittee, thank you for the privilege to appear before you today. It's an honor to appear alongside CISA's Executive Assistant Director for Cybersecurity Eric Goldstein. I am eager to share with you what the Office of the National Cyber Director (ONCD) is doing to mature the public-private partnership with industry to better secure critical infrastructure from cyber intrusions, including destructive cyber attacks. The Biden-Harris Administration continues to strengthen our cybersecurity defenses and prepare our Nation with unprecedented focus, and the ONCD is proud to work alongside our interagency partners in these efforts.

The President has taken aggressive action to secure the Nation's critical infrastructure and is prepared to use every tool to deter, disrupt, and when appropriate, respond to cyberattacks against our homeland. In May 2021, the President issued Executive Order 14028, mandating extensive cybersecurity measures for the Federal Government to ensure we are leading by example. The ONCD, working with our partners at the Office of Management and Budget (OMB) and the National Security Council, is conducting implementation oversight of Executive Order 14028, to ensure continued progress on fulfilling the Order's requirements.

Since the fall 2021, as Russian President Vladimir Putin escalated his aggression against Ukraine, the Biden-Harris Administration has worked to provide extensive briefings and advisories to U.S. businesses and individuals regarding potential threats and the cybersecurity measures they can put in place to protect themselves. CISA, the FBI, the National Security Agency's Cybersecurity Directorate – and, in many cases, our international partners – have issued numerous threat advisories outlining Russia's malicious intent and activities in cyberspace and outing their tools and infrastructure. The professionals in our Intelligence Community have done outstanding work in exposing Putin's nefarious plots, while our cyber defenders continue to ensure strategic warnings are paired with actionable steps for companies and the American public to defend themselves.

Recognizing the unique risks presented in cyberspace for the conflict to spill out of Ukraine and onto our shores, the federal government has also partnered with industry on tabletop exercises, bringing important critical infrastructure stakeholders – including CEOs – together to operationalize collaboration and prepare for various scenarios. Paired with classified intelligence read-ins and aggressive declassification efforts, these exercises help enhance resilience and coherence among our private sector partners, Federal departments and agencies. The Administration has also been able to leverage relationships developed through public-private action plans under the President's Industrial Control Systems Cybersecurity Initiative to enhance the cybersecurity posture of the electricity, pipeline, and water sectors.

On March 21, 2022, the President reiterated his warning about potential cyber attacks from Russia against critical infrastructure and urged companies to harden cyber defenses immediately and deploy best practices. The government and private sectors must also continue to work together to build national resilience and productively collaborative to address and defeat the evolving cyber threats we face. The Administration has prioritized stronger cybersecurity controls for critical infrastructure sectors where we have authority to do so and is creating innovative public-private partnerships and initiatives to enhance cybersecurity across all our critical infrastructure. Congress has partnered with us on these efforts, and we appreciate the bipartisan work of this Committee to require companies to report cyber incidents to the United States Government. These efforts have become even more critical as we assess evolving intelligence that Russia may be exploring options for potential cyber attacks on U.S. critical infrastructure.

The ONCD is helping to execute the Biden-Harris Administration's cyber agenda by, among other things, working to improve public-private collaboration in cybersecurity. Through strategic engagements with stakeholders, the ONCD is establishing and maintaining relationships to enhance knowledge sharing and strategic coordination and collaboration. ONCD is working with the NSC, other White House components, and relevant agencies to harness the once-in-a-generation scope and scale of the Infrastructure Investment and Jobs Act to build infrastructure that is future-proofed and resilient to cyber threats, with standards and policy frameworks necessary for a durable cyber foundation.

As we work with industry to invest in the resiliency of our infrastructure, we remain committed to rapidly improving our collaboration with industry to address today's cyber threats. We work closely with our federal partners, including CISA, OMB, the Department of Justice, including the FBI, the National Institute of Standards and Technology (NIST), and Sector Risk Management Agencies (SRMAs) to expand engagement and partnership opportunities across sectoral lines and increase collaboration.

CISA has a central role to play in building our capacity for collaboration with the private sector. I expect that EAD Goldstein will highlight CISAs ongoing efforts in this area to mature collaboration and improve cybersecurity, but let me highlight one critical success. CISA leveraged the authority entrusted to it by Congress to establish the Joint Cyber Defense Collaborative (JCDC), an organization that brings together representatives from government and industry collaborating to identify threats, develop crisis response plans, and foster the relationships needed to quickly share information and respond to malicious cyber-incidents. The JCDC has already had some early successes, most notably by bringing government and the private sector together to respond to the Log4j vulnerability. Building resilience to potentially catastrophic cyber-incidents will require an unprecedented level of planning, information sharing, and operational collaboration. Efforts to connect government and industry experts, such as the JCDC, can identify and address threats far more effectively than can any single organization operating alone.

Equally important, however, is the role of SRMAs, each a vital component of the Federal governments capacity to assist private sector entities in improving cybersecurity. SRMAs have statutory responsibilities to work with their sectors on a day-to-day basis and help surface information relevant to other sectors and are vital for managing national risk. Agencies like the Department of Energy, the Department of the Treasury, and others are partnering closely with industry to share information, drive risk management activities, and collaborate to reduce risk. Sector Coordinating Councils and organizations like ISACs and ISAOs have been proven to be useful mechanisms for information sharing, but we need to mature the policies and procedures for strengthening collaboration. NSA's Cybersecurity Collaboration Center, in partnership with the Defense Industrial Base Sector, is an example of the power of bringing together cyber threat experts and network defenders to enable more secure Department of Defense (DoD) and defense industry platforms and systems.

Resourcing SRMA functions, including those resident at CISA, is key to achieving the Federal coherence that is central to the strategic intent of the ONCD. ONCD is beginning an initiative to review the cyber capabilities and resources of SRMAs and understand the requirements to operationalize SRMAs so that they can better collaborate in cyber defense. As part of this review, ONCD is examining current authorities and a pilot program that can be used to mature these efforts. We are also examining how we can improve internal government capacity to collect and share threat intelligence with these entities.

We also need to strengthen our efforts to coordinate law enforcement capabilities with private sector entities to combat botnets, ransomware and other malicious activity. The Department of Justice, including the FBI, has enjoyed a string of successes in disrupting ransomware operations. ONCD is reviewing opportunities to create linkages to further mature the ability to coordinate these efforts with private sector entities that may be targeted by threat actors or have information or capabilities that can support government action.

Congress, Presidential policy, the Department of Homeland Security, and SRMAs have long recognized the need to identify critical infrastructure that if successfully targeted by adversaries could cause disproportionate harm to the American people and the U.S. economy. Section 9 of Executive Order 13636 requires the Secretary of Homeland Security to identify critical infrastructure where a cybersecurity incident could reasonably result in catastrophic effects on public health or safety, economic security, or national security. In March 2020, the Cyberspace Solarium Commission proposed a "designation of critical infrastructure entities that manage systems and assets whose disruption could have cascading, destabilizing effects on U.S. national security, economic security, and public health and safety." These entities support National Critical Functions and are of heightened interest to nation-state adversaries. Given the potential consequences of a cyber incident impacting a Section 9 entity, there is a vested interest of both the federal government and the private sector to improve the security and resilience of these entities.

The Administration supports the general concept of identifying systemically important entities that own, operate, or otherwise control critical infrastructure. ONCD is evaluating how to enhance the Federal government's capacity to reduce the risk to National Critical Functions posed by adversaries against the entities that own and operate our most important systems and assets and to understand and improve their resiliency to cyber attacks. Specifically, we are examining authority and capacity to provide prioritized support to, and opportunities to collaborate with, these entities, as well as the possibility for tailored obligations required on designated entities. Additionally, CISA is currently developing a plan and timeline for the rulemaking required under the Cyber Incident Reporting for Critical Infrastructure Act, or "CIRA". We look forward to working with Congress to ensure that any potential framework for systemically important entities is complementary to CIRA and other ongoing efforts across the Administration.

Finally, one of the most important things that we can do to mature the public-private partnership to secure U.S. critical infrastructure is to make sure we are extracting lessons learned from cyber incidents and implementing those lessons as rapidly as possible. The Biden-Harris Administration created the Cyber Safety Review Board (CSRB) modeled after the National

Transportation Safety Board with the goal of reviewing significant cyber incidents with this purpose in mind. Established in accordance with Section 5 of Executive Order 14028, the Board brings together government and private sector leaders to analyze significant cybersecurity incidents, generate lessons learned, and produce concrete recommendations to avoid future crises. Director Inglis proudly serves on the Board, which is currently undertaking a review of the vulnerabilities in the Log4j library that came to light last December. I am also actively engaged in the review. Importantly, following this first review, the CSRB will review its own processes and develop plans for improving future reviews.

With the continued support of the President and the Congress, the Office of the National Cyber Director is committed to building robust relationships with industry and our interagency partners to enhance the security and resilience of our Nation's cyber ecosystem. Thank you for the opportunity to testify before you today, and I look forward to your questions.

*** END ***