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

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

April 6, 2022

Washington, D.C.

Chairwoman Clarke, Ranking Member Garbarino, and members of the Subcommittee, thank you for the opportunity to testify today on behalf of the Cybersecurity and Infrastructure Security Agency (CISA) regarding our efforts to evolve our partnerships with the private sector to enable true operational collaboration.

In our globally interconnected world, our critical infrastructure and American ways of life face a wide array of serious risks with significant real-world consequences. Today, the critical functions within our society are built as "systems of systems," complex designs with numerous interdependencies and systemic risks that can have cascading effects. This trend has yielded significant gains in efficiency and productivity, but also provides the opportunity for nation-state actors and criminals to potentially undermine our national security, economic prosperity, and public health or safety.

The risks we face today are complex and dispersed, both geographically and across a variety of stakeholders. They are challenging to assess and difficult to address. Consequently, we must recognize that threats to our digital infrastructure are not bound by national borders. Rather, our critical infrastructure is integrated into a larger global cyber ecosystem requiring us to be at the constant ready.

This committee is well aware of CISA's broader domestic role as the operational lead for federal cybersecurity, and as the national coordinator for critical infrastructure security and resilience. The importance of CISA's mission and role has been clearly reflected during the war in Ukraine, as we have led the nation's efforts across government and the private sector to prepare for potential malicious cyber activity by Russian actors.

Critical to our success, and at the heart of CISA's mission, is partnership and collaboration. Securing our Nation's cyber and critical infrastructure is a shared responsibility and has never been more important than it is today. Neither government nor the private sector have the knowledge or resources to do it alone. At CISA, we are challenging traditional ways of doing business and are actively working with our government, industry, academic, and international partners to change the paradigm from traditional public-private partnerships to public-private operational collaboration at scale. Operational collaboration is foundational for effective critical infrastructure security and resilience. Timely, trusted information fusion among stakeholders is essential.

In the past year, CISA has made significant strides in this respect, particularly through the establishment of the Joint Cyber Defense Collaborative (JCDC) and our CISA Cybersecurity Advisory Committee (CSAC). These groups are examples of CISA's agency-wide dedication to operational collaboration and deep partnership, which is imbued across our mission divisions. By leveraging the expertise and unique authorities of government and the private sector, CISA is better positioned to connect with our stakeholders in industry and government to share resources, analyses, and tools. This in turn helps our stakeholders build their own cyber, communications, and physical security and resilience. The net effect is a stronger Nation, better positioned to contend with the myriad threats we face to our cybersecurity and critical infrastructure.

As we strive to make progress in the security of our Nation's critical infrastructure through our various partnership initiatives, we are not looking to duplicate the efforts of the private sector. Instead, CISA is looking for ways we can add value, such as bringing experts from government and industry together, compiling a broader holistic view of the cyber landscape, and sharing information across sectors to ultimately make our Nation's critical infrastructure resilient against malicious cyber activity.

Our work has taken on increased urgency subsequent to Russia's unprovoked invasion of Ukraine. CISA has been working closely with our critical infrastructure partners over the past several months to ensure awareness of potential threats. We have been providing additional resources, guidance, and support for months, and reiterated this call for critical infrastructure to adopt a heightened security posture in light of President Biden's statement that intelligence shows Russia may be exploring options for potential cyberattacks. As part of our broader "Shields Up" effort, we developed and published a variety of resources, including guidance for organizations, corporate leaders and CEOs, individuals, ransomware response, and a list of additional resources, multiple joint Cybersecurity Advisories (CSAs), mitigation guidance, including recent products on securing satellite communications and uninterruptible power supply devices, and a dedicated Technical Guidance web page with mitigation guidance and resources from CISA, the JCDC and other partners. Our goal with all of these efforts is to serve as a comprehensive resource for information about mitigations for the Russian cyber threat.

Joint Cyber Defense Collaborative (JCDC)

Given that the vast majority of our Nation's critical infrastructure is owned and operated by the private sector, the early warnings of a cyber-attack affecting U.S. organizations are more likely to be identified by a private company rather than the government. The private sector plays a vital role in working with CISA to improve our nation's cyber security by helping to ensure that we are aware of new campaigns or intrusions so we can protect other possible victims.

Critical to CISA's effort to build better operational collaborative channels is the JCDC, which leverages authorities granted in the FY2021 NDAA, among other authorities, and was launched by CISA in August 2021 to lead collaborative, public and private sector cyber defense planning, cybersecurity information fusion and analysis, and the purposeful dissemination of cyber defense guidance to reduce cyber risks to the Nation's critical infrastructure and the impact to our National Critical Functions (NCF).

Today, the JCDC is a collection of more than 25 private sector companies working with CISA and other federal government cybersecurity partner agencies – including DHS Office of Intelligence and Analysis, FBI, NSA, U.S. Cyber Command, the U.S. Secret Service, and relevant Sector Risk Management Agencies (SRMA) – to understand and respond to cyber threats. The diversity and unique capabilities of JCDC partners provides increased visibility and insight into the threat landscape and enables JCDC to develop plans and exercises against the most serious threats.

The JCDC model reflects the reality that no one entity can secure cyberspace alone. Collaboration across JCDC partners results in action across an expansive set of cybersecurity stakeholders throughout the nation and the globe.

By leveraging and unifying the respective capabilities, authorities, and expertise of the JCDC's partners, CISA is creating a proactive, rather than reactive, capability for the government and private sector to work together to drive down risk even before an incident occurs. Should another incident like the compromises affecting SolarWinds Orion, Microsoft Exchange Server, or Colonial Pipeline occur, the strengthened connective tissue among our partners will allow for a more unified response.

The JCDC operating model relies on regular analytic and data exchanges to enable common situational awareness and equip public and private sector partners to take risk-informed coordinated action for our collective defense. Simply put, the work of the JCDC is about seeing the dots, connecting the dots, and collectively driving down risk to the nation at scale. This alignment strengthens our mutual resilience and ability to address immediate and impending cyber incidents. Collaborative insights gleaned from the JCDC are then rapidly shared across the broader cybersecurity community, including through our Cybersecurity Information Sharing and Collaboration Program and through a broad ecosystem of Information Sharing and Analysis Centers (ISACs) and Organizations (ISAOs).

In its short history, the JCDC has strengthened the lines of communication between industry and the federal government to improve real-time information sharing, planning, and exercising. For example, when CISA issued its emergency directive in response to the Log4j vulnerability, CISA leveraged the JCDC, establishing a senior leadership group within the the organization to coordinate collective action and ensure shared visibility into both the prevalence of the Log4j vulnerability and threat activity. By bringing together key government and private sector partners via the JCDC, including the agency's partners at the FBI and the NSA, CISA was able to ensure that the country's strongest capabilities were brought to bear in an integrated manner against the threat.

Having built trust and strengthened relationships with our partners during our response to the Log4j incident, the JCDC was well prepared to respond to the current dynamic threat environment amidst rising geopolitical tensions related to the Russia-Ukraine war.

To ensure domestic resilience against potential cyber-atacks in response to the Russia-Ukraine war, the President designated the Department of Homeland Security as the Lead Federal Agency (LFA) for domestic preparedness and response related to the current crisis. Secretary Mayorkas then established a Unified Coordination Group (UCG) and appointed CISA's Executive Director to serve as the Senior Response Official to ensure federal unity of effort across the U.S. government. The stand-up of the UCG formalized the work CISA had been doing for months with Sector Risk Management Agencies (SRMAs) to inform stakeholders of the heightened threat environment, and conduct intelligence-based threat briefs for SRMA partner agencies, Sector and Government Coordinating Councils, and participants from the private sector and state and local community. In addition, CISA is working with FEMA, SRMAs and other federal partners to manage downstream physical consequences of potential cyber attacks. The Russia-Ukraine crisis has brought on a whole-of-government and whole-of-nation preparedness effort

More broadly with the private sector though, the JCDC has served as a critical forum to implement standing operational collaboration channels.

For example, CISA developed a Russia-Ukraine crisis plan with our JCDC partners that lays out phases and objectives of operational coordination between the U.S. Government and our private sector partners amidst escalating geopolitical tensions. In mid-February, we conducted a tabletop exercise of this plan with our interagency and private sector partners. We are using the plan as tensions escalate to guide and align our collective operational posture and support our ability to esynchronize defensive actions to mitigate harmful impacts to US critical infrastructure from Russian cyber operations. In the wake of distributed denial of service (DDoS) and destructive malware attacks affecting Ukraine and other countries in the region, we are working very closely with JCDC and international cyber defense partners to understand and rapidly share information on these ongoing malicious cyber activities.

Moreover, JCDC's collaborative channels have allowed CISA to exchange technical information about recent incidents in Ukraine and conduct real-time analysis with interagency and industry partners. Further still, the JCDC established additional information sharing mechanisms with the nation's largest energy and financial companies, in coordination with the appropriate SRMAs, allowing CISA to provide additional early warning about Russian activity against U.S. institutions and exchange related threat information and defensive measures.

We recognize that many critical infrastructure partners or SLTT governments find it challenging to identify resources for urgent security improvements. In response, JCDC has worked with our partners to compile a list of free cybersecurity tools and services to help organizations further advance their security capabilities. This catalog includes CISA's own services, open-source tools, and free offerings from private sector entities, including our JCDC partners. The catalog includes resources like malware and antivirus protection systems, vulnerability assessment solutions, tools that test password strength, distributed denial of service protection services and intelligence from several leading cybersecurity companies. This is particularly impactful for small businesses and SLTT organizations who are target rich and resource poor.

Going forward, we continue to build and mature the JCDC construct. We are particularly focused on advancing our capability to create, exercise, and execute joint cyber defense plans. Upcoming planning efforts focus on the energy sector and collaboratively supporting defense of the nation's election infrastructure. The JCDC has demonstrated the promise of a new model for public-private operational collaboration: joint cyber planning—including deliberate and crisis action plans—through collaboration across the public and private sectors to prepare for and address the nation's most pressing cyber risks, combined with integrated and institutionalized testing and assessments to continuously measure and improve the effectiveness of cyber defense planning and capabilities.

Through these collaborative efforts, we will enable common situational awareness, information fusion, and analysis that equips public and private partners to take risk-informed coordinated action. This journey is not CISA's alone. Rather, we are embarking on a rapid evolution in concert with our partners across the inter-agency and private sector, with a shared goal of advancing our nation's security and resilience at scale.

Systemically Important Entities (SIE)

Through our operational collaboration efforts, we have learned that prioritization is essential. By focusing on systemic risks, growing interdependencies within and across sectors and our evolving reliance on information and communications technology (ICT), we will more effectively reduce the potential of cascading impacts associated with the failure of these technologies that could threaten our national and economic 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."[1] At CISA, we are operationalizing this concept by developing approaches to identify Systemically Important Entities (SIE). These are entities that own, operate, or otherwise control critical infrastructure, prioritized based on indicators of systemic importance and the potential impact that their disrupted or corrupted functions will have a debilitating, systemic or cascading impact on our country's critical infrastructure and related NCFs, national security, national economic security, public health, public safety, or some combination thereof.

As the private sector owns and operates a vast majority of the Nation's critical infrastructure, partnerships like JCDC, CSAC, and others that foster integrated, collaborative engagement and interaction are essential to maintaining critical infrastructure security and resilience. Therefore, identifying systemically important private sector firms, in addition to SLTT and other public entities, is paramount to prioritizing the partnerships CISA establishes and maintains to reduce risk to critical infrastructure.

To aid in this identification, CISA established an SIE effort within the National Risk Management Center (NRMC) to develop the SIE concept in order to prioritize CISA's delivery of services to those entities. CISA's SIE effort, which seeks to support and respond to partners and stakeholders across the federal government, private industry, and SLTT governments, will be the central body responsible for coordinating across CISA, DHS, and the interagency to manage stakeholder engagement with systemically important entities. Additionally, CISA is sponsoring work by the Homeland Security Operations Analysis Center (HSOAC) to develop a prototype analytic capability to identify SIEs at scale. By using advanced data-analytic techniques that evaluate entities based on their network centrality and sector revenue, we will be better able to identify and assess an SIE's importance across the NCFs and close gaps in their risk profiles.

Identifying SIEs is more than just a naming and mapping exercise. By identifying SIEs we will be better positioned to understand the true landscape of institutions and systems whose disruption could have cascading and systemic effects to our critical infrastructure and related NCFs. This knowledge will better position us to prioritize these entities for CISA services and capabilities and identify mature entities whose partnership can help the Nation reduce systemic risk to our cyber and critical infrastructure.

[1] United States of America. (2020). *Cyberspace Solarium Commission, Final Report*. p. 138. Retrieved from https://www.cybersolarium.org/reports-and-white-papers

While we are committed to growing our capacity to collaborate and share information, CISA and our federal partners are limited in our ability to influence private sector functions, such as complex supply chains, that are an increasing source of cyber risk. Fortunately, SIEs can help set expectations for acceptable activities and behavior by employing effective supply chain security risk management practices.

CISA will prioritize partnership and engagement with the SIE community and provide recommendations for addressing the emerging challenges of systemic risk. We particularly would benefit from specific input from partners regarding our efforts to improve our understanding of systemic risk.

The SIE program is of critical importance. While we are committed to protecting all of the nation's critical infrastructure, not all infrastructure is created equal. Assets and systems that are of such vital importance to our security require prioritized protection in collaboration with the private sector. In some cases, individual companies can reduce risk because they own or operate a significant portion of the assets and systems. CISA's efforts to begin the identification process of systemically important entities represents a vital, and necessary, first step in that process.

CISA Cybersecurity Advisory Committee (CSAC)

Even as we work through the JCDC to collaborate around urgent risks of today and develop cyber defense plans to address those risks still ahead, we must also learn from diverse minds across the cybersecurity community to advance CISA's strategic maturation. To achieve this goal, we recently launched the CISA Cybersecurity Advisory Committee (CSAC), a key authority granted in the National Defense Authorization Act (NDAA) for Fiscal Year 2021.

The CSAC was established with the purpose of bringing together strategic thinkers with diverse expertise and insights to examine issues and create recommendations related to the development, refinement, and implementation of policies and programs that will help to advance the cybersecurity mission of CISA as well as strengthen the cybersecurity of the United States. In December 2021, Director Easterly appointed 23 leading experts on cybersecurity, technology, risk management, privacy, and resilience from across industry, academia, and government to serve as the CSAC's initial members. The diversity of the Committee's members emphasizes the need for an "all hands-on deck" approach to secure our digital networks.

CSAC members advise, consult with, report to and make recommendations to the Director on the development, refinement, and implementation of policies, programs, planning, and training pertaining to CISA's cybersecurity mission. The Committee will examine and make recommendations on a variety of topics collectively aimed at strengthening CISA and more broadly reshaping the cyber ecosystem to favor defense. These topics include growing the cyber workforce; reducing systemic risk to national critical functions; combating misinformation and disinformation impacting the security of critical infrastructure; and turning the corner on cyber hygiene by raising the baseline of security throughout the cyber ecosystem to advance an environment that favors the defender by better aligning government and private sector efforts to build resilience and improve cyber hygiene at scale. In addition, the CSAC recently established a new Technical Advisory Council, a subcommittee of the CSAC, with some of the most accomplished individuals in the cybersecurity community to provide CISA with expert insights into advancing our collaboration

with the research community and ensuring that our programs reflect leading technology practices.

Building on the momentum from the Committee's inaugural meeting in December, the CSAC convened again just this past week on March 31st. Protecting the Nation's critical infrastructure depends on a unified effort and we remain committed to ensuring that we have the right strategy in place to prepare for, respond to, and mitigate cybersecurity threats to our Nation's critical systems. CISA looks forward to the recommendations made by the Committee members and the subsequent subcommittees.

Cyber Safety Review Board (CSRB)

A continuous learning culture is critical to staying ahead of the increasingly sophisticated cyber threats we face in today's complex technology landscape. Recognizing this need, President Biden's Executive Order 14028 on *Improving the Nation's Cybersecurity* directed DHS to establish a Cyber Safety Review Board (CSRB) to review significant cyber incidents to ensure that the nation fully understands and learns from significant cyber events that may threaten us all.

The CSRB serves a deliberate function to review major cyber events and make concrete recommendations that would drive improvements within the private and public sectors. As a uniquely constituted advisory body, the CSRB will focus on learning lessons and sharing findings with the President, and with others who can benefit from them, as appropriate.

The private sector has a significant role to play in providing visibility, validation, and insight into how cyber events emerge and which short and long-term improvements can stave off future, similar events, and incidents. The CSRB – composed of 15 highly esteemed cybersecurity leaders from the federal government and the private sector – provides a unique forum for collaboration between government and private sector leaders who will deliver strategic recommendations to the President and the Secretary of Homeland Security.

Conclusion

Our nation is at a turning point in cybersecurity. We must continue to work together, by deepening our operational collaboration and ensuring we have the plans and policies in place now, to defend against new and changing cyber threats going forward. Recent incidents and the ongoing threat of malicious Russian cyber activity provide a stark reminder about the vulnerability of our country's critical infrastructure. The need for increased risk sharing and distribution between the government and private sector is clear.

The cyber ecosystem is a shared space with shared responsibilities and shared benefits, with every organization gaining from the interoperability, scale, and resilience of the internet and networked technologies. As a result, every organization must invest in protecting it. Together we can address the risks we all face. CISA's public and private sector programs provide novel collaborative venues for diverse entities to evolve their relationships.

Now is the time to act – and CISA is helping to lead our national call to action. We will deepen our partnerships with critical infrastructure partners, enhance our visibility into national cybersecurity, and drive targeted action to reduce vulnerabilities and detect our adversaries. In

collaboration with our government partners, critical infrastructure entities, our international allies, and with the support of Congress, we will make progress in addressing this risk and maintain the availability of critical services to the American people under all conditions.

****END****