CISA CYBERSECURITY ADVISORY COMMITTEE
SEPTEMBER 13, 2022, MEETING SUMMARY

OPEN SESSION

Call to Order and Welcoming Remarks

Ms. Megan Tsuyi, Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Advisory Committee (CSAC) Designated Federal Officer, called the meeting to order. She reviewed the *Federal Advisory Committee Act* rules governing the meeting and noted that while the Committee advertised the opportunity for public comment there had been no requests from the public to provide comment.

The Hon. Jen Easterly, CISA Director, welcomed the attendees and briefly reviewed the background and intent of the CSAC. The Director announced the completion and distribution of CISA's Strategic Plan for 2023 - 2025. She then asked Mr. Brandon Wales, Executive Director, CISA, to introduce the four pillars of the plan.

Operational Updates

Mr. Wales provided a high-level overview of the CISA Strategic Plan. He reflected on the overall mission focusing on the resiliency and security of the Nation's critical infrastructure. He highlighted the four pillars approach of the CISA Strategic Plan: 1) spearhead efforts to make a more resilient cyberspace; 2) determine how to reduce risks and strengthen the Nation's critical infrastructure; 3) ensure close operational coordination and information sharing; and 4) determine how to make CISA a more effective and efficient organization. Mr. Wales reiterated that the CISA Strategic Plan is a starting point for CISA moving forward over the next three years.

Director Easterly described CISA's effort to align Agency goals and objectives with specific measurements that help reduce risk. She pointed out that the Strategic Plan highlights many of the undertakings CISA accomplished since its establishment, including the launch of the Shields Up campaign. Director Easterly then asked Mr. Eric Goldstein, Executive Assistant Director for Cybersecurity, CISA, to provide an operational update.

Mr. Goldstein stated that CISA remains vigilant against threats, even though the Nation has not suffered a major cyber-attack. He cited the recent major cyber intrusions across the globe, including the recent attack in the Albanian government, Great Britain, and the prevalence of ransomware attacks across the globe. He provided an overview of CISA objectives, including promoting steps entities may take to bolster their own security and readiness. He emphasized the recent cross-sector discussion to share information to establish best mitigation practices to secure networks independently.

Mr. Goldstein announced the launch of the Joint Ransomware Task Force, established by Congress and co-chaired by CISA and the Federal Bureau of Investigation (FBI), and its goal to reduce the impact of ransomware by cross-sector collaboration to determine best practices of tackling the emergent threat of ransomware intrusion. He continued with a review of CISA's Cybersecurity Awareness Month.

Director Easterly introduced Mr. Tom Fanning, CSAC Chair, Southern Company to provide opening remarks and lead the discussion through the seven Subcommittee updates.

Mr. Fanning welcomed CSAC Members and expressed his gratitude for their work on the CSAC. He emphasized the importance of CSAC's recommendations to the Nation's future, and significant value produced by the discussions surrounding these issues. He clarified the schedule of the session and opened the floor for opening comments to Mr. Ron Green, CSAC Vice Chair, Mastercard.

Mr. Green reflected that CSAC has made tremendous strides over the past year collaborating between the public and private sector. He shared his enthusiasm for CSAC's continued achievements and recommendations to bolster the efficiency and resiliency of the Nation's cybersecurity.

Subcommittee Updates

Building Resilience and Reducing Systemic Risk to Critical Infrastructure

Mr. Fanning thanked the **Building Resilience and Reducing Systemic Risk to Critical Infrastructure** (SR) Subcommittee members and credited the individuals who contributed to the SR Subcommittee's report to the CISA Director.

Mr. Fanning summarized the three pillars in the SR report: 1) the "who" pillar identifies systemically important entities (SIEs); 2) the "what" pillar specifies resiliency goals for orderly and efficient action; and 3) the "how" pillar details programs and structures that enable resiliency goals. He reviewed key findings from the SR Subcommittee's research, including the significant disparity in maturity levels of SIEs, the importance of shared national goals, the need to avoid economic calamity, and the value in harmonizing cyber regulations. He encouraged CISA to consider replacing Executive Order 13636 Improving Critical Infrastructure Cybersecurity Section 9 entities with the SIEs.

Mr. Fanning reviewed the SR recommendations within each pillar:

1. Identify SIEs. Collaborate with the private sector on shared obligations. Engage SIEs to identify risk derivatives, coordinate cross-sector risks, and prioritize responses to emerging risks based on impact. Prepare SIEs for triage capabilities.

2. Develop a common framework with shared language and goals. Create a culture that unifies CISA, sector risk management agencies, the intelligence community, the private sector, and other national stakeholders.

3. Establish goals. Construct an analytic framework with baseline risk management. Provide a forum for business partners to identify their assets and practices. Build an integrated approach to resilience and a maturity model that evaluates performance. Address the perspectives of system owners and operators in addition to their Chief Executive Officers and Chief Information Security Officers. Leverage existing regulations and avoid duplication. Focus on outcomes rather than processes. Demonstrate the value of participation.

Ms. Lori Beer, JPMorgan Chase, thanked the SR Subcommittee's subject matter experts. She expounded on the value of collaboration within the financial industry. She recognized the government's ability to provide unique capabilities to the private sector.

Ms. Marene Allison, Johnson & Johnson, explained that some industries have already organized themselves, and others would benefit from the frameworks (e.g., Information Sharing and Analysis Centers [ISACs]) that deliver national insights).

Mr. Kevin Mandia, Mandiant, advocated for a test, respond, remediate, and repeat cycle to identify deficiencies and improve the work product. He emphasized the importance of testing and operationalizing recommendations within the third "how" pillar.

Mr. Fanning informed the group that the SR Subcommittee conducted two tabletop exercises during its information gathering stage.

Mr. Green remarked that transparent goals would incentivize companies to correct their own issues before a regulator prompts the company to take corrective actions. Mr. Fanning agreed with the comment, and he mentioned that transparency is iterative.

Mr. Ted Schlein, Kleiner Perkins, thanked the SR Subcommittee members for their work. He asked about the message to entities that pay taxes and want access to the government even though they are not SIEs. Mr. Fanning responded that the SIE designation enables asset prioritization, real-time evaluation of the cyber battlefield, consistent responses, and valuable feedback loops to share the SIEs' lessons learned with other entities via the

ISACs. He acknowledged that there may be timing differences (e.g., declassification of information), but he concluded that everyone would benefit from these recommendations.

Ms. Nicole Wong, NWong Strategies, asked if the Transforming the Cyber Workforce (TCW) and SR Subcommittees should work together to address talent gaps. Mr. Fanning encouraged collaboration between all CSAC Members.

Director Easterly applauded the SR Subcommittee's comprehensive work on the report and recommendations. She underscored the importance of their work for CISA's core mission and its ongoing efforts to collaborate, reduce risk, measure outcomes. Director Easterly described several no-cost services that CISA publishes for non-SIEs. She acknowledged the usefulness of the SIE designation in responding to and recovering from major cybersecurity incidents.

CSAC Members voted on and unanimously approved the recommendations.

Protecting Critical Infrastructure from Misinformation and Disinformation

Ms. Suzanne Spaulding, Center for Strategic and International Studies, thanked **Protecting Critical Infrastructure from Misinformation and Disinformation (MDM)** Subcommittee Chair Dr. Kate Starbird, University of Washington, for her leadership and reviewed that she would lead the Subcommittee's update in Dr. Starbird's absence. Ms. Spaulding briefly summarized the Subcommittee's focus on addressing the urgent risk facing U.S. elections and election officials. She upheld that elections have a critical national function to faithfully reflect the will of the people and secure a peaceful transition of power.

Ms. Spaulding reviewed that the recommendations emphasize the need for CISA to focus on threats to U.S. elections and election officials. Such threats manifest in two ways: 1) cyber-enabled threats designed to reduce public trust in the legitimacy of the elections process; and 2) broader mis- and dis-information operations the public continues to see. The recommendations aim to help CISA better support state and local election officials dealing with both types of threats. She reviewed the key findings from the MDM Subcommittee's work to ensure CISA coordinates directly with the Intelligence Community (IC), including the FBI, to prioritize the needs of election officials and identify intelligence requirements at a local level. Subcommittee members suggest CISA contact election officials to identify current needs. She noted that the recommendations are affirmed by state and local election officials themselves.

Ms. Spaulding reviewed the second set of recommendations that advise CISA to help the courts ensure the resolution of disputes and the peaceful transfer of power, as the courts have become a significant target of mis- and dis-information attacks. The Subcommittee expanded on the earlier set of recommendations presented during the CSAC June Quarterly Meeting. The Subcommittee emphasized CISA's role to provide resources, best practices, templates, and website guidance to state and local election officials to give them the tools needed to proactively address mis- and dis-information. The Subcommittee suggested CISA leverage its far-reaching platform by amplifying state and local resources on its communications channels. Ms. Spaulding stressed that elections must be managed at the local level by local election officials, but upheld CISA's role to provide needed resources. Regarding threats from foreign adversaries, the report recommended that CISA promptly share information from the IC with state and local election officials.

Director Easterly thanked the Subcommittee for their work and stressed that CISA is committed to remaining non-partisan and non-political as the Agency works with every state and local election official to address the concern of how mis- and dis-information impacts election operations. She reaffirmed CISA's commitment to upholding civil rights and civil liberties that are at the core of the American democracy. She reviewed CISA's actions to date in this space to include the CISA Joint Cyber Defense Collaborative (JCDC)'s toolkit of free election security resources tailored to election officials. She further emphasized that CISA's role is not to run elections, but to share resources with election officials. She detailed CISA's focus to empower election officials to manage threats through coordinated vulnerability discovery and disclosure support, working with state vendors on disclosure programs, providing physical security including insider threat guidance, and releasing associated trainings online for rapid

access. Director Easterly commended the Subcommittee for their focus on supporting work with the courts.

Mr. Schlein suggested CISA remove the wording of mis- and dis-information due to its politicization. He recommended framing discussions around CISA's work providing the American people with accurate information.

CSAC Members voted on and unanimously approved the recommendations.

Turning the Corner on Cyber Hygiene

Mr. George Stathakopoulos, Apple, identified the **Turning the Corner on Cyber Hygiene** (CH) Subcommittee's focus and security requirements. Mr. Stathakopoulos noted that the Subcommittee centered their original efforts on targeting small and medium organizations, places that cannot provide their own IT security and cyber hygiene. This idea has since expanded to include the entire spectrum of organizations.

Mr. Stathakopoulos reviewed the CH Subcommittee's previous recommendation for CISA to focus on Multi-Factor Authentication (MFA). He encouraged CISA to saturate the cybersecurity landscape with this message as much as possible and partner with large companies to amplify this message. He suggested that large companies could also pledge their support to encourage other organizations to enable MFA. He detailed the Subcommittee's earlier recommendation for CISA to support and expand upon the Austin 311 pilot program which has been tested already.

Mr. Bobby Chesney, University of Texas, described the current partnership University of Texas, Austin, and the City of Austin has with various private sector entities. He campaigned for the need to scale up the required talent to enact a national partnership and solicit inquiries on how that might be possible. He submitted that the goal was pioneering a direct intersection between various cities and CISA, to establish partnerships. Mr. Stathakopoulos added that CISA should use metrics gathered through the partnership in Austin, Texas to determine emergent CISA partnerships.

Mr. Stathakopoulos opened the floor to comments and questions from the attendees. Ms. Marene Allison, Johnson & Johnson, noted that it might be more effective to focus messaging senior corporate (C-Suite) executives and resiliency forums, as opposed to only Chief Security Officers. Ms. Nuala O'Connor, Walmart, responded that the recommendations are pointed toward all C-Suite executives. Mr. Green added that it would be beneficial to push these recommendations to boards of directors as well. Director Easterly clarified the importance of a robust cyber ecosystem to all boards of directors, as cyber security is business security.

Mr. Stathakopoulos added that the next step would be to find new potential targets and centralize partnerships.

Director Easterly stressed that cyber risk is business risk is national risk. She also expressed support for the idea of a cyber hotline.

Transforming the Cyber Workforce

Mr. Green thanked the **Transforming the Cyber Workforce** (TCW) Subcommittee members and reviewed the TCW Subcommittee's ongoing assessment of curricula, candidate qualifications, and service requirements for people who participate in the government's cybersecurity programs. He discussed efforts to attract cybersecurity talent, to identify pipelines that match talent with opportunities at CISA, to research cyber skills, and to evaluate the availability of apprenticeships and mentorships. Mr. Green addressed upcoming efforts to study the decentralized workforce and propose recommendations at the CSAC December Quarterly Meeting.

Mr. Chris Young, Microsoft, commented on the relationship between the TCW Subcommittee's work and other CSAC Subcommittee's initiatives. He identified the cyber skillset as a common denominator, and he noted the potential for collaboration.

Director Easterly announced that CISA's new Chief People Officer (CPO) will join in October 2022. She asserted that the CPO would help to unify these efforts. Ms. Kiersten Todt, Chief of Staff, CISA, summarized an initiative between the Department of Commerce, Department of Labor, the National Institute of Standards and Technology, and CISA to promote cyber apprenticeships and job retraining. Mr. Green indicated that the TCW Subcommittee would include that initiative in its research.

Strategic Communications

Ms. Niloofar Razi Howe, Tenable, thanked the **Strategic Communications** (SC) Subcommittee members. Ms. Howe commended CISA on their various outreach and newly released Strategic Plan that imparts unity of effort, unity of message, and practical details that support cybersecurity practitioners.

Ms. Howe reviewed the SC Subcommittee's contributions to several CISA initiatives, including the CISA.gov website redesign. Ms. Howe elaborated that the website must reflect the mission and goals of CISA, starting with a complete redesign. She addressed CISA's unique challenge to serve myriad stakeholders with a broad range of perspectives. She affirmed the SC Subcommittee's support for future iterations of the website. Ms. Howe also offered the SC Subcommittee's support for any approved CSAC recommendations.

Ms. Nicole Perlroth, Cybersecurity Journalist, added that the SC Subcommittee sees itself as a partner to the other CSAC Subcommittees and that it is prepared to support in any way possible.

Technical Advisory Council

Mr. Eric Goldstein, CISA, briefed on the **Technical Advisory Council** (TAC) Subcommittee's efforts in the absence of Subcommittee Chair Mr. Jeff Moss, DEF CON Communications. He affirmed the Subcommittee's support of the recommendations accepted by the full Committee during the CSAC June Quarterly Meeting regarding vulnerability discovery and disclosure and cyber threat intelligence sharing. He reviewed the Subcommittee's actions to date to include meeting with stakeholders across critical infrastructure and state, local, territorial, and tribal governments for additional context on how CISA interacts with key partners and to inform the group's next set of recommendations. He thanked the Subcommittee members for their work reviewing CISA's guidance to small businesses and reviewing challenges in reaching critical threat areas.

Director Easterly affirmed the significant level of support the TAC Subcommittee members have given CISA by providing feedback on ways to engage small businesses.

Closing Remarks and Adjournment

Director Easterly thanked the CSAC Members for their attendance and contribution to the discussion. She announced that the next CSAC Quarterly Meeting will be on December 6, 2022.

Director Easterly informed the Committee that CISA is working through the recommendations from the CSAC June Quarterly Meeting. She stated that CISA will finalize its response by October 6, 2022. She elaborated that the response will explain how the Agency plans to implement the recommendations, and that it will be consistent with the CISA Strategic Plan released on September 13, 2022. Director Easterly also introduced Ms. Lisa Einstein, CSAC Executive Director, CISA, and stated that her role would be to help bolster the CSAC's work.

Mr. Fanning thanked everyone for their recommendations and commitment to refining the work that the CSAC has produced. He acknowledged the Committee's role in producing meaningful results and improving cybersecurity outcomes for the U.S. He encouraged each member to be aspirational in their thinking, and he conveyed his excitement and appreciation for the CSAC's work.

Mr. Fanning adjourned the September Quarterly Meeting.

APPENDIX: CLOSED SESSION PARTICIPANT LIST

CSAC Members	Organization
Marene Allison	Johnson & Johnson
Lori Beer	JPMorgan Chase
Bobby Chesney	University of Texas School of Law, Austin
Tom Fanning	Southern Company
Ron Green	Mastercard
Niloofar Razi Howe	Tenable
Kevin Mandia	Mandiant
Jeff Moss	DEF CON Communications
Nuala O'Connor	Walmart
Nicole Perlroth	Cybersecurity Journalist
Ted Schlein	Kleiner Perkins
Steve Schmidt	Amazon
Suzanne Spaulding	Center for Strategic and International Studies
Alex Stamos	Krebs Stamos Group
George Stathakopoulos	Apple
Nicole Wong	NWong Partners
Chris Young	Microsoft

Government Participants	Organization
Director Easterly	CISA
Alaina Clark	CISA
Victoria Dillon	CISA
Lisa Einstein	CISA
Trent Frazier	CISA
Eric Goldstein	CISA
Mona Harrington	CISA
Nitin Natarajan	CISA
Jen Pedersen	CISA
Kiersten Todt	CISA
Megan Tsuyi	CISA
Brandon Wales	CISA
Kim Wyman	CISA

CSAC Support	Organization
Mariah Bailey	Edgesource
Jonathan Dunn	CISA
Lisa Einstein	CISA
James Eustice	Edgesource
Mariefred Evans	TekSynap
Sonja Grant	CISA
Nayeema Hoq	CISA
Celinda Moening	CISA
Lauren Rousseau	Edgesource
Barry Skidmore	CISA
Xavier Stewart	Edgesource

Other Attendees

Other Attendees	Organization
Karin Athana	TIC Council Americas
Mariam Baksh	Government Executive Media Group
Robert Barton	Plains All American Pipeline, L.P.
Ashley Billings	CNN
Pascal Boctor	Cornerstone Government Affairs
Ian Brown	CISA
AmyClaire Brusch	Airports Council International – North America
Ross Clark	CISA
Anne Disse	Apple
Justin Doubleday	Federal News Network
Adrienne Dowling	CISA
Mathew Eggers	US Chamber of Commerce
Kelly Feili	Depository Trust and Clearing Corporation
Ben Flatgard	JPMorgan Chase
Amy Flowers	Microsoft
Bree Fowler	CNET
Benjamin Freed	StateScoop/EdScoop
Sara Friedman	Inside Cybersecurity
Will Garrity	Mastercard
Elizabeth Gauthier	CISA
Eric Geller	Politico
Kegan Gerard	Southern California Edison
Mardy Goote	Software & Information Industry Association
Aileen Graef	CNN
Jonathan Greig	The Record
Michele Guido	Southern Company
Judith Harroun-Lord	Transportation Security Administration
Gabe Hengel	CISA
Gwainevere Hess	CISA
Joey Hewitt	Plains All American Pipeline
Nicole Hodziewich	Lockheed Martin
Kathryn Ignaszewski	IBM
Abi Kinnard	Cornerstone Government Affairs
Norma Krayem	Van Scoyoc Associates
Navid Kreshavarz-Nia	Raytheon Technologies Corporation, Raytheon Intelligence & Space
Danouh Louis	CISA
Jerry Markon	MeriTalk
Alexandra Martin	CISA
Scott McConnell	CISA
Jennifer McGrath	Unum Law
Devi Nair	Center for Strategic and International Studies
Stacy O'Mara	Mandiant
Theresa Paraschac	Depository Trust and Clearing Corporation
Jacob Phillips	MISO
Dylan Presman	Office of the National Cyber Director
Katheryn Rosen	JPMorgan Chase
Geneva Sands	CNN
Robert Schill	Blackberry
Cedric Sharps	TekSynap
Jordana Siegel	Amazon
Samuel Spector	Blackberry
Claire Teitelman	JPMorgan Chase

September 13, 2022

Other Attendees (Cont.)	Organization
Erik Thomas	Systems Engineering
Liz Turrell	CNN
Christian Vasquez	E&E News
Keith Woolford	Siemens DIS

CERTIFICATION

I hereby certify that, to the best of my knowledge, the foregoing minutes are accurate and complete.

Tom Fanning (approved on 12 October 2022)

Mr. Tom Fanning
CISA Cybersecurity Advisory Committee Chair
October 12, 2022