CISA CYBERSECURITY ADVISORY COMMITTEE
June 22, 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 there were no requests for public comment.

Director Jen Easterly, CISA, welcomed the attendees and thanked Mayor Steve Adler, Austin, Texas, and Mr. Bobby Chesney, Dean Designate, University of Texas Austin Law School, for hosting the CSAC June Quarterly Meeting. Director Easterly updated the committee on actions CISA has taken since the CSAC Kickoff Meeting in December 2021 to include mitigating the risk of the Log4Shell vulnerability, CISA's actions in response to Russia's invasion of Ukraine, strengthening the Shields Up campaign, and the Joint Cyber Defense Collaborative (JCDC). Director Easterly expressed gratitude to members for their advice and counsel to respond to the initial taskings with thoughtful and creative recommendations. Director Easterly outlined the path forward in responding to the recommendations within 90 days and emphasized her full commitment to transparently sharing how CISA would implement those recommendations.

She reviewed the CSAC's new tasking focused on the feasibility of an alert system for cyber risk to ensure the nation is not operating at a Shields Up, highest posture of alert, at every moment. She reviewed the cyber advisory threat alert system tasking which will target businesses large and small and offer very specific, actionable steps.

Director Easterly applauded the work of the subcommittees to date and welcomed Mr. Tom Fanning, CSAC Chair, Southern Company, to provide opening remarks.

Mr. Fanning welcomed CSAC Members and expressed his gratitude to members for their work on the CSAC. He emphasized that not only are the CSAC's recommendations themselves important to the country's future, but the discussions surrounding these issues will produce a significant value.

Mr. Ron Green, CSAC Vice Chair, Mastercard, reflected that the recommendations were a direct result of the CSAC's commitment to the cybersecurity mission. He commented that he was encouraged by what the members were able to accomplish and what each subcommittee continues to do.

Mr. Fanning confirmed with Ms. Tsuyi that there is a public comment period, but there are no public comments to discuss. He outlined the agenda for the afternoon session to designate approximately 20 minutes of discussion per subcommittee to include updates and any items for full CSAC vote. Mr. Fanning turned the meeting over to Mr. Green for his updates on the Transforming the Cyber Workforce Subcommittee.

Subcommittee Updates

Transforming the Cyber Workforce

Mr. Green emphasized the **Transforming the Cyber Workforce** Subcommittee's commitment to their work. The subcommittee's recommendations were broken down into two categories: CISA's workforce challenges and national challenges.

In addressing CISA's workforce challenges the CSAC recommends that CISA prioritize strategic workforce development, dramatically improve its talent acquisition process to be competitive with the private sector, radically expand recruitment efforts to identify candidates across their professional lifecycle, and leverage talent identification and hiring success through interagency collaboration. He commended CISA for taking the initial steps to hire a Chief People Officer.

He noted that CISA must dramatically improve hiring goals and processes and recommended that CISA lower the hiring timeframe to 90 days to delivery of a Temporary Job Offer (TJO). He reviewed the suggestion for CISA to develop a systemic approach to collecting and analyzing data on candidate pools and hiring processes, review hiring goals with senior leadership, and move to more flexible and manageable results.

Mr. Green stressed that closing the agency's talent gap will require rapidly expanding recruitment efforts. Current recruiting pools do not encompass the entire spectrum of talent. To improve hiring practices, CISA should establish a standard working group to advise on best practices, utilize guidance from public and private sector advisors, and expand internship opportunities to recruit emerging talent. He encouraged CISA to conduct these actions through a thorough review of the interagency security clearance process and develop a senior leader specific hiring strategy. Director Easterly asked Mr. Green to have the subcommittee review the Agency's security clearance process to determine ways to better streamline it.

Mr. Green emphasized the need for creative, new programs which would lower the barrier of access into cyber security positions. He noted the recent establishment of CISA's Cyber Innovation Fellows as one great example. The committee suggests that CISA open a cyber academy which will partner with the private sector and community colleges and universities along with other industry supported cyber education providers, develop a cyber security training curriculum which will be taught at academic institutions, and unify the cyber oriented programs under one junior cyber corps umbrella.

The committee recommended CISA establish a cyber force program and a peace corps like cyber program. This program would provide education and service to provide domestic security development assistance.

Director Easterly thanked the subcommittee for their ambitious and actionable recommendations. She commended the subcommittee for providing actionable recommendations.

CSAC Members unanimously approved the recommendations.

Turning the Corner on Cyber Hygiene

Mr. George Stathakopoulos, Apple, identified the **Turning the Corner on Cyber Hygiene** Subcommittee's focus and security requirements. He shared the recommendation that CISA build out its current multi-factor authentication (MFA) campaign by identifying additional vehicles for publicizing "More Than a Password", take all available steps to ensure that companies working with the federal government fully adopt MFA by 2025, and that CISA launch a "311 National" campaign that provides an emergency call line and clinics for assistance with cyber incidents for small and medium businesses. He encouraged CISA to make the recommendations clear and attractive and make it easier for companies to receive the help they need.

Mr. Chesney recommended that CISA partner with cities and universities to complete the "311 National" line. Mr. Stathakopoulos noted that the recommendations are the initial steps in a long journey towards securing the American public and businesses. He stressed the need for over-saturation in that CISA should amplify cyber hygiene messaging across all audiences and communications forums.

Mr. Eric Goldstein, CISA, added that accessing talent pools within cities and universities might allow CISA to deploy talent, such as computer science and engineering students or law and business students, to work for credits or pro bono in clinics.

CSAC Members provided feedback on the recommendations. Mr. Green commended the subcommittee on the simplicity of their approach to the MFA campaign by helping the average person. Mr. Fanning stated that he is

encouraged by the subcommittee's systemic thinking.

Director Easterly expressed her excitement for "More Than a Password" and noted that they launched the campaign at the RSA Conference in the beginning of June. She also thanked the subcommittee for their idea of a local partnership and Mayor Adler for volunteering to use Austin as a pilot.

CSAC Members unanimously approved the recommendations.

Technical Advisory Council

Mr. Jeff Moss, DEF CON Communications, reviewed the composition of the **Technical Advisory Council** (TAC) Subcommittee and detailed the two recommendations on coordinated vulnerability discovery and disclosure (CVD) and cyber threat intelligence (CTI).

Mr. Moss explained the CVD recommendations are externally focused and detailed the difficulties in reporting vulnerabilities. He stressed that CISA, as the nation's cyber defense agency, can make the reporting process more attractive. He noted that the researcher community has limited time and energy to report vulnerabilities and the more complicated the process, the less likely they will report a detected vulnerability. He encouraged CISA to develop incentives and access to information to aid security researchers who will submit vulnerabilities affecting critical systems. CISA should work to enable a frustration-free CVD process by working with Congress and sector-specific regulatory agencies to require that manufacturers supply firmware images of every released version for the industry, which should ultimately be archived for future automated analysis. He urged CISA to invest in a central platform to facilitate the intake of suspected vulnerabilities and communication between security researchers, agencies, and vendors. While the Vulnerability Information and Coordination Environment (VINCE) is not the prescribed solution, Mr. Moss recommended that CISA adapt a system similar to VINCE. Mr. Moss recommended that CISA simplify the reporting process and provide feedback to those reporting.

Mr. Moss reviewed the second, internally facing recommendation on CTI and shared the impression that CISA is doing well in this area, but the recommendations feature overall observations on areas of improvement. He recommended that CISA automate this process to start with the users most in need. He recommended that CISA invest in a program to make CTI available to all qualified users and eliminate barriers to access such as high costs. This would significantly benefit smaller organizations in need of additional CTI assistance. CISA should also invest in enriching CTI reports to increase durability across all layers of defense. He also encouraged CISA to explore techniques to enable scalable and effective development of expertise in CTI.

Mr. Goldstein noted the recommendations would be extraordinarily impactful in enhancing CISA's ability to act as a trusted broker of the CVD process to work collaboratively with vendors to reduce the risk of exposure.

Mr. Fanning asked Mr. Moss to clarify how he envisioned a frustration-free reporting process. Mr. Moss reflected on a briefing from the Food and Drug Administration to note the wide range in complexities throughout each sector's reporting process. He stressed that CISA can provide value by vetting information to determine who the vulnerability affects so it is clearly communicated and alleviates the work of the researcher.

Ms. Nicole Wong, NWong Strategies, suggested that CISA consider posing these recommendations to the Cyber Innovation Fellows program Director Easterly is establishing. Mr. Chris Young, Microsoft, underscored the importance of CISA's role in the CVD process to bridge the wide gap in complexities between sectors and organizations.

CSAC Members unanimously approved the recommendations.

Protecting Critical Infrastructure from Misinformation and Disinformation

Dr. Kate Starbird, University of Washington, highlighted the difficulty of the **Protecting Critical Infrastructure from Misinformation and Disinformation Subcommittee's** tasking in today's complex environment. She recommended that CISA take the same action in response to countering mis-, dis-, and mal-information (MDM) as the Agency does to counter cyber threats. She defined the scope of the recommendations in the elections context and

emphasized the expressed need from elections officials from all political parties to do this work, given the acute struggle of elections officials—especially those in small jurisdictions—to address and understand MDM threats. She noted that MDM threats undermining trust in the elections process has led to physical threats against elections officials, reaching the highest level of death threats and attempts to enact harm. Dr. Starbird recommended that CISA focus on informing the public on MDM threats and partner with frontline elections officials to inform the public and point to first-hand elections resources from Secretaries of State. She emphasized that CISA should not prescribe any messaging, but rather point to resources from the state-level.

Dr. Starbird reviewed the four MDM recommendations to CISA. She encouraged CISA to follow a resilience-based approach to launch a broad public awareness campaign on MDM to enhance individual and collective resilience. The campaign should include civics education to understand how to identify MDM and build an understanding of why citizens should not want to spread MDM. She noted that this aligns with CISA's cyber hygiene mission. Dr. Starbird encouraged CISA to proactively address anticipated MDM threats through education. This response should be in the form of pointing to trusted and authoritative sources of information at the local level—in particular, local election officials. She encouraged CISA to rapidly respond to emerging threats in a transparent manner. Dr. Starbird suggested that CISA identify, communicate, and respond to actor-based threats.

She encouraged CISA to support local elections officials by convening a "What to expect on election day" workshop to provide a platform for elections officials themselves to share best practices. She noted the subcommittee's path forward to continue to work through the more challenging questions.

Ms. Alicia Tate-Nadeau, Illinois Emergency Management Agency, emphasized the expressed need from elections officials for guidance on how to counter MDM threats. She stressed that the recommendations are focused on providing tools to elections officials so that they themselves can develop their own best practices.

Ms. Suzanne Spaulding, Center for Strategic and International Studies, reinforced Dr. Starbird's points and thanked her for her leadership. She recognized that public trust is essential in this work and stressed the urgent need to support state and local elections officials.

Director Easterly noted that CISA is beholden to supporting and defending the Constitution and helping to safeguard free and fair elections as the Sector Risk Management Agency for election infrastructure security is part of that mission. She underscored that the federal government's role is not to run elections, but to provide support and resources to every state and locality to help them ensure the security and resilience of elections. Dr. Starbird highlighted Ms. Kim Wyman's, CISA, participation in the subcommittee as a former Republican Secretary of State. Dr. Starbird shared a quote from Mr. Steven Richer, Maricopa County Recorder, Georgia, that "responding to misinformation is my day job. My night job is running elections.". She stressed that the subcommittee's work is focused on supporting elections officials from all parties across the country. Director Easterly again stressed the criticality of transparency and maintaining trust with the American people.

Mr. Fanning commended Dr. Starbird on her work.

CSAC Members unanimously approved the recommendations.

Building Resilience & Reducing Systemic Risk to Critical Infrastructure

Mr. Fanning reviewed the **Building Resilience & Reducing Systemic Risk to Critical Infrastructure** Subcommittee's actions to examine CISA's work on the concept of Systemically Important Entities (SIE) and the Agency's efforts to enhance resilience across the nation's 55 National Critical Functions (NCFs). He explained that the subcommittee developed two tabletop exercises (TTXs) simulating cyberattacks on the generate electricity NCF to inform their recommendations that will be made to CISA during the CSAC September Quarterly Meeting. He detailed the goal of the TTXs is to break down risk to identify interdependencies and gaps to target systemic risk.

Mr. Fanning stated that the subcommittee will now focus on collaboration responses and how to integrate with the JCDC, the Federal Emergency Management Agency, and State, and Local governments.

Mr. Kevin Mandia, Mandiant, added that the TTXs will help CISA iron out communication issues before a threat arrives.

Director Easterly noted the evaluation of risk on critical infrastructure is a core mission of CISA. She thanked the subcommittee and expressed her excitement to receive their recommendations in September.

Strategic Communications

Ms. Niloofar Razi Howe, Tenable, reviewed the goal of the **Strategic Communications** Subcommittee to enhance CISA's strategic communications efforts, outreach, and partnerships. She reflected on the subcommittee's success partnering with other CSAC Subcommittees to improve their effectiveness and help drive outcomes.

Two of the recommendations were in support of the Turning the Corner on Cyber Hygiene Subcommittee to include the More Than A Password campaign and the Austin 311 Pilot. Regarding the "More Than A Password" campaign, Ms. Howe encouraged CISA to designate a program manager to work with Fortune 500 companies to define their commitment to providing resources, establishing metrics to drive success, and develop a full campaign around cyber hygiene. Regarding the Austin 311 Pilot, Ms. Howe encouraged CISA to create a playbook to identify the process to enable a nationwide program rollout with as little friction as possible.

Ms. Howe recommended that CISA build a broader base of support. She applauded CISA for building trust and support with partners and stakeholders and encouraged CISA to build upon this strength by bringing in cyber reporters for regular briefings. She highlighted the importance of expanding CISA's list of Agency validators to secure allies and amplifiers before CISA news is released. This is an opportunity to build trust and confidence in the U.S. Government's work more broadly.

Director Easterly affirmed the importance of the subcommittee's work, as many members of the public are unaware of CISA's core mission. She thanked the subcommittee for partnering with other efforts and for recruiting cybersecurity journalists. She flagged that the CISA Cybersecurity Awareness Month is approaching in October and this will present additional opportunities for the subcommittee.

CSAC Members unanimously approved the recommendations.

Closing Remarks and Adjournment

Mr. Fanning thanked CSAC Members for their diligence and thoughtfulness in crafting the recommendations. Director Easterly restated her gratitude to the members for developing specific, actionable recommendations.

Mr. Fanning reminded public participants that a meeting summary will be available on the CSAC website and reminded members that the next CSAC Quarterly Meeting is scheduled for September 13, 2022. Mr. Fanning adjourned the meeting.

APPENDIX: OPEN SESSION PARTICIPANT LIST

CSAC Members	Organization
Mr. Steve Adler	City of Austin, Texas
Ms. Marene Allison	Johnson & Johnson
Mr. Robert Chesney	University of Texas
Mr. Thomas Fanning	Southern Company
Ms. Vijaya Gadde	Twitter
Mr. Ron Green	Mastercard
Ms. Niloofar Razi Howe	Tenable
Mr. Kevin Mandia	Mandiant
Mr. Jeff Moss	DEF CON Communications
Ms. Nicole Perlroth	Cybersecurity Journalist
Mr. Matthew Prince	Cloudflare
Ms. Suzanne Spaulding	Center for Strategic and International Studies
Dr. Kate Starbird	University of Washington
Mr. George Stathakopoulos	Apple
Ms. Alicia Tate-Nadeau	Illinois Emergency Management Agency
Ms. Nicole Wong	NWong Strategies
Mr. Chris Young	Microsoft

Government Participants	Organization
The Hon. Jen Easterly	CISA
Ms. Alaina Clark	CISA
Ms. Victoria Dillon	CISA
Ms. Stephanie Doherty	CISA
Mr. Jonathan Dunn	CISA
Mr. Eric Goldstein	CISA
Ms. Mona Harrington	CISA
Mr. Bob Lord	CISA
Ms. Celinda Moening	CISA
Mr. Johnathan Moor	CISA
Ms. Jennifer Pederson	CISA
Mr. Harvey “PT” Perriott	CISA
Mr. Kris Rose	CISA
Mr. Rob Russell	CISA
Mr. Taylor Smith	CISA
Ms. Kiersten Todt	CISA
Ms. Megan Tsuyi	CISA
Ms. Kim Wyman	CISA

Contractor Support	Organization
Ms. Mariefred Evans	TekSynap
Ms. Marissa Pope	EdgeSource
Ms. Thais Price	TekSynap
Mr. Xavier Stewart	EdgeSource

In-Person Participants	Organization
Mr. Brett DeWitt	Mastercard
Ms. Anne Disse	Apple
Mr. Benjamin Flatgard	JPMorgan Chase
Ms. Michele Guido	Southern Company
Mr. Gary Luedecke	City of Austin, Texas
Ms. Devi Nair	Center for Strategic and International Studies
Ms. Stacy O'Mara	Mandiant
Ms. Jordana Siegel	Amazon Web Services

Dial-In Participants	Organization
Ms. Mariah Bailey	TekSynap
Ms. Mariam Baksh	Nextgov
Mr. Calvin Biesecker	Defense Daily
Mr. Scott Bouboulis	Wiley Rein LLP
Ms. Dana Bostian	Bostian Captioning
Mr. Evan Burke	U.S. House of Representatives
Ms. Emily Burns	U.S. House of Representatives
Ms. Cynthia Brumfield	Metacurity
Mr. Jack Cable	HSGAC
Ms. Sarahjane Call	DHS
Mr. Chris Cook	Appropriations - U.S. Senate
Mr. Joseph Chilbert	Office of Partnership Engagement
Mr. Cameron Dixon	CISA
Mr. Justin Doubleday	Federal News Network
Mr. Luiz Eduardo	Aruba Threat Labs
Mr. Matt Eggers	U.S. Chamber of Commerce
Ms. Lisa Einstein	Federation of American Scientists
Mr. Michael Feldman	CISA
Mr. Matthew Fleisher-Black	The Cybersecurity Law Report
Ms. Amy Flowers	Microsoft
Mr. David Forscey	CISA
Ms. Sara Friedman	Inside Cybersecurity
Mr. Matthew Gasser	TSA

Dial-In Participants (Cont.)	Organization
Ms. Elizabeth Gauthier	CISA
Mr. Eric Geller	Politico
Ms. Aileen Graef	CNN
Ms. Sonja Grant	CBP
Ms. Carmen Hadgraft	Southern Company
Ms. Gwen Hess	CISA
Mr. Edward Humphrey	CISA
Mr. Zachary Isakowitz	U.S. House of Representatives
Mr. Adam Israelevitz	U.S. House of Representatives
Mr. Alexander Jacobs	DHS
Mr. David Jones	Cybersecurity Dive
Mr. Albert Kammler	Van Scoyoc Associates
Mr. Matt Kehoe	Apple
Ms. Norma Krayem	Van Scoyoc Associates
Ms. Christina Lee	Beacon Global Strategies
Mr. Tom Leithauser	Telecommunications Reports and Cybersecurity Policy Report
Ms. Oumou Ly	CISA
Mr. Joseph Marks	Washington Post
Mr. Martin Matishak	The Record
Ms. Neysa Matthews	Walmart
Mr. Glenn Merell	Freelance Consulting
Mr. Mike Miron	DHS
Mr. Phu Nguyen	Integrated Cybersecurity Engine
Mr. Andrew Nicholson	Imperium Global Advisors
Mr. Jeff Rothblum	U.S. Senate
Ms. Sophia Salome	CISA
Mr. Jason Sanford	Illinois Emergency Management Agency
Mr. Aaron Schaffer	Washington Post
Mr. Robert Sheldon	CrowdStrike
Ms. Jenny Shore	CISA
Mr. Tim Starks	CyberScoop
Mr. Travis Stoller	Wiley Rein LLP
Ms. Claire Teitelman	JPMorgan Chase
Mr. Christian Vasquez	E&E News
Mr. Shaun Waterman	Waterman Reports
Ms. Leah Young	CISA

CERTIFICATION

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

Tom Fanning (approved on 21 July 2022)

Mr. Tom Fanning
CISA Cybersecurity Advisory Committee Chair