CISA CYBERSECURITY ADVISORY COMMITTEE
MARCH 31, 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 provided a short summary of *Federal Advisory Committee Act* rules governing the meeting and then turned the meeting over to CISA Director Jen Easterly.

Director Easterly welcomed the attendees and introduced the Committee's Chair, Mr. Tom Fanning, Southern Company, and Vice Chair, Mr. Ron Green, Mastercard. 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, preparing for potential cyber threats emerging from Russia's unjust invasion of Ukraine, launching CISA's Shields Up campaign, and promoting a message of preparation, not panic, in the face of potential cyber-attacks on our critical infrastructure. Director Easterly highlighted the cyber incident reporting legislation and omnibus budget passed to increase CISA's overall funding. Director Easterly reiterated her gratitude for the Committee's feedback and counsel during this challenging operational environment.

Director Easterly commented on CISA's efforts to build trusted and collaborative partnerships with industry and highlighted the importance of the Joint Cyber Defense Collaborative (JCDC)'s work and her intent to scale this model to include more partners and broader collaboration to maximize the benefits to the cybersecurity community. Director Easterly then mentioned the ongoing debate about the need for more regulation in critical infrastructure. She offered her recognition for the value of implementing minimum standards for cybersecurity, but also noted concerns about overly burdensome and unharmonized regulations which can result in compliance box-checking rather than real operational risk reduction. Director Easterly stated the goal of the cyber incident reporting is to add value, not burden, and to make CISA a better partner to industry by increasing transparency and information sharing in a way that prevents future attacks while also protecting the privacy and anonymity of the victim.

Director Easterly applauded the work of the subcommittees to date and welcomed Mr. Fanning to provide opening remarks. Mr. Fanning and Mr. Green thanked Director Easterly and Committee members for their participation and noted the criticality of the subcommittee's work to strengthen our nation's cybersecurity resilience.

Subcommittee Updates

Transforming the Cyber Workforce

Mr. Green emphasized the subcommittee's focus on closing the cyber talent gap for CISA and the Nation. He reviewed the subcommittee's work on helping CISA to develop a human capital strategy, talent pipelines, and retention programs to advance prospective individuals into the cyber industry.

Mr. Green outlined the subcommittee's progress thus far to include conversations with CISA leadership, employees who have gone through the hiring process, hiring managers within CISA, individuals responsible for successful hiring initiatives within the government sector, and other outside organizations that have an interest in helping the nation advance its cybersecurity pipeline. Through these discussions, the subcommittee will consider recommending that CISA shorten the interview process that can take up to six months and implement a sustainable education grant program to develop unrealized talent in underserved communities. Mr. Green stressed that the connective tissue between operational teams at CISA and the private industry needs to be strengthened.

CSAC members discussed the importance of collaboration between public and private sectors to strengthen CISA's hiring efforts. Mr. Fanning noted the difference between attracting employees versus retaining them. In terms of industry and government collaboration, Mr. Green shared the idea of Intergovernmental Personnel Appointments (IPA) to allow the agency to bring individuals from the private sector to serve in a governmental capacity. Mr. Fanning noted that at least 85 percent of the critical infrastructure industry is privately owned, making collaboration necessary to CISA's success. Mr. Ted Schlein, Kleiner Perkins Caufield & Byers, recommended introducing a rapid response team for cyber where CISA can pull together a group of experts quickly to solve a particular problem, then send recommendations back to industry quickly, in comparison to what was described as the IPA program. Mr. Green noted that this idea is not something the subcommittee has explored yet, but it is something they will discuss.

Director Easterly noted the recent deployment of the Cyber Talent Management System (CTMS) which has allowed for more flexibility in reducing the steps to onboarding. Director Easterly recommended that the subcommittee receive a full update on CTMS and provide their feedback to determine if this resolves onerous onboarding issues.

Turning the Corner on Cyber Hygiene

Mr. George Stathakopoulos, Apple, identified the subcommittee's focus as finding a way to simplify security recommendations to small and medium businesses. This aligns with the subcommittee's path forward to execute a holistic, scaled approach to ensure that all organizations have the information and resources needed to implement essential security practices. Due to the limited security resources of small businesses, Mr. Stathakopoulos specified small businesses as the most vulnerable to a potential attack, which could have larger implications across an entire sector. Mr. Stathakopoulos detailed six basic steps for businesses to implement to include: (1) hold trainings; (2) implement multi-factor authentication (MFA); (3) patch known vulnerabilities; (4) enable logging on current system; (5) build an incident response plan; and (6) strengthen cyber resilience. He identified a goal for the subcommittee to impart an amplified message of "More Than A Password" to promote MFA implementation. Mr. Stathakopoulos described the path forward to build coalitions and present these recommendations to Fortune 500 companies, non-profits, and universities. Mr. Stathakopoulos added the subcommittee's second goal is to examine the possibility of an emergency call line for ransomware attacks.

CSAC members discussed ways to strengthen the effectiveness of the outlined recommendations. Members proposed potential incentives for businesses that implement these security strategies ranging from the tax incentives recommended by Mr. Schlein to eliminating the existing "MFA tax," as suggested by Mr. Alex Stamos, Krebs Stamos Group. Mayor Steve Adler, City of Austin, identified areas of collaboration with the Strategic Communications Subcommittee to strengthen the broad messaging efforts. Ms. Nuala O'Connor, Walmart, concurred that this is a joint communications and education effort for small and medium businesses and agreed with the focus on simplifying the security message. Mr. Chris Young, Microsoft, asked the subcommittee to consider small businesses operating on a non-cloud infrastructure and the security issues associated with non-cloud operating platforms.

Technical Advisory Council

Previously known as the Igniting the Hacker Community, Mr. Moss, DEF CON Communications, stated the Technical Advisory Council subcommittee is focused on a broader community than just hackers to further catalyze CISA's relationship with the technical community to shift the balance in favor of network defenders. He identified CISA's difficulty interacting at the individual level and called out the community's lack of trust in organizations and true trust in people. Mr. Moss encouraged CISA to build and maintain trust with the researcher community at a person-to-person level. He stated the subcommittee's efforts to determine the best ways for CISA to ignite the power of the technical community from all backgrounds and experiences to create a trusted partnership with the government and CISA. Mr. Moss detailed the subcommittee's path forward to incentivize and reduce barriers to vulnerability reporting and outlined a range of initiatives on expanding collaboration with the technical community, including hackers, academics, and researchers. Such ideas included easing the reporting process and building web portals for individuals to report incidents online. Finally, he identified the subcommittee's immediate interest in determining what specific problems CISA is aiming to solve.

Committee members offered examples of best practices within their fields and posed questions to Mr. Moss on potential areas for the Technical Advisory Council to consider. Ms. Suzanne Spaulding, Center for Strategic & International Studies, inquired if the subcommittee had discussed the role of transparency in terms of building trust with the government to openly communicate how the government is using the insights shared by this community. Ms. Spaulding expressed a concern of over-classification by the government as a barrier to reporting. Mr. Moss said the subcommittee is also considering the role of the Civil Liberties and Privacy Community in such an effort and agreed with Mr. Fanning and Mr. Schlein on the importance of transparency in building trust. Ms. Marene Allison, Johnson & Johnson, provided an example of incident reporting best practices in the healthcare sector.

Mr. Eric Goldstein, Head of CISA Cyber, outlined another goal of the subcommittee as to understand this community's perceptions about working with government to understand and remove any deterring factors. He added that CISA's goal is also to unpack incentive models around reporting vulnerabilities to CISA in order to drive more effective and regular disclosure. In thinking about incident reporting accountability among CEOs as part of the business control environment, Director Easterly and Mr. Fanning asked the subcommittee to consider developing a guide for board directors on questions they should be asking about cyber security reporting.

Protecting Critical Infrastructure from Misinformation and Disinformation

Dr. Kate Starbird, University of Washington, discussed the subcommittee's actions to date and path forward to confront mis-, dis-, and malinformation (MDM) harmful to critical infrastructure. Dr. Starbird noted the subcommittee is focused on using strategies to prevent MDM during elections to provide a blueprint on targeting MDM in other contexts, and continues to question how CISA can best support the MDM mission. By focusing on elections, Dr. Starbird stated that the subcommittee can examine CISA's mission across four main areas to include: (1) civics and media literacy— enhancing societal resilience to MDM; (2) proactive work of narrative-specific staging of resources and pre-bunking; (3) response through monitoring, identifying, and addressing specific MDM threats; and (4) detect and respond to foreign influence operations. Dr. Starbird outlined the subcommittee's path forward of determining how CISA can participate effectively in election truth narratives and how CISA can build trust within this adversarial space.

Committee members highlighted the focus of MDM as undermining the overall trust in government. Mr. Green offered the recommendation that CISA target already trusted communities within the adversarial space to increase CISA's credibility. Ms. Niloo Razi Howe, Energy Impact Partners, concurred that pre-bunking MDM before it spreads is imperative in this context. She added that increasing transparency and rapidly declassifying information are ways CISA can build alliances to deter bad actors. Committee members noted that operational collaboration is a significant way to combat MDM. Ms. Howe offered to connect the subcommittee to resources outside the academic community working on pre-bunking resources.

Building Resilience & Reducing Systemic Risk to Critical Infrastructure

Mr. Fanning shared that the subcommittee is determining how to best drive national risk management and identify the criteria for scalable, analytic models to prioritize risk. He addressed one of the group's challenges as understanding the bridge between the National Risk Management Center (NRMC) and how to incorporate this work into the JCDC. He noted that the subcommittee is reimagining the notion of national security, focusing on collaborations between the private sector and government to ensure they are not thinking of critical risk sectors in a silo. Mr. Fanning applauded the NRMC for their work examining the national critical functions (NCFs) and the interdependencies among sectors to ensure a sound response to a major incident. He stated that the subcommittee is focused on determining the highest priority NCFs and evaluating realistic scenarios at the asset level. Mr. Fanning shared that the subcommittee is determining recommendations that could be potentially operationalized into policy and law, and how to best define CISA's charge for protecting our critical infrastructure. Mr. Fanning mapped out the subcommittee's path forward to examine specific NCFs including (1) generate electricity, particularly examining risks to pipelines; (2) water; (3) financial services; and (4) telecommunications to then develop scenarios which will explore the impacts at the asset and supply chain levels to determine the corresponding effects of an attack and how collaboration between industry and government can best secure America. Following the scenarios, the subcommittee

will develop a playbook on how to communicate this collaboration.

CSAC members discussed CISA's role in sector risk management without recreating cybersecurity capabilities extensively within other governing departments and agencies. Director Easterly commented that CISA is not looking to replace Information Sharing Analysis Centers (ISACs), but is rethinking ways to share relevant data. Mr. Goldstein commented that sector risk management agencies (SRMAs) provide expertise in sector-specific risks and an understanding of how to expand function resilience within sectors under all conditions. In cyber intrusions, CISA is able to provide generalized cyber expertise which can be applied, combined with the sector-specific knowledge of the SRMAs to drive down risk across sectors at scale. Mr. Goldstein shared that the JCDC is focused on how to generalize and scale the current risk models to increase operational collaboration across sectors as novel risks are identified. This will lead to a force multiplier effect to drive down risk far more quickly than companies can accomplish individually.

Chris Inglis, National Cyber Director, provided an overview of the Office of the National Cyber Director's (NCD) mission to assess the performance of cyber investments including the roles and responsibilities, not just financial investments. He shared that the NCD is currently performing a study in partnership with CISA on the SRMAs to determine recommendations for further action to get each of them up to the level of performing tabletop exercises.

Ms. Allison concluded the subcommittee's updates by highlighting that interconnectivity breeds actionable intelligence and stressed the need to strengthen the partnership between government and industry.

Strategic Communications

Ms. Howe reviewed the subcommittee's task of addressing how CISA can communicate their mission in a way that engages stakeholders around risk management issues. She stated the subcommittee's second focus of exploring how CISA can improve communications to ensure all audiences are informed of CISA's mission and value add to the nation's cyber defenses. She outlined the path forward and current challenges of the subcommittee to include how to be most effective in communicating CISA's mission.

Ms. Howe suggested the subcommittee reconvene to build partnerships between each subcommittee. Ms. Howe identified two action items for the subcommittee, to include (1) identifying the next step as receiving a brief on CISA's longer term strategic communications strategy and (2) receive a brief from each subcommittee chair to determine how the subcommittee can support, develop, and boost communication needs of the Committee as a whole.

Committee members discussed ways to more clearly identify the subcommittee's messaging efforts regarding CISA's mission and value add. Ms. Nicole Perlroth, Cybersecurity Journalist, suggested to conceptualize CISA's messaging in two ways, (1) thinking of the CISA brand itself and (2) how to educate others regarding cyber hygiene. Director Easterly emphasized the importance of CISA being responsive to all feedback and how that directly correlates with the public trusting the Federal Government.

Mr. Fanning thanked the participants for their comments and turned the meeting over to Ms. Tsuyi for the Public Comment Period.

Public Comment Period

Mr. Joe Weiss, Applied Control Solutions, LLC, provided the following comment for the record:

> Thank you for this opportunity to provide comment. My comments I think will cover a number of the working groups and it's dealing with engineering considerations. Process sensors and operational technology (OT) networks are used in every physical infrastructure, everything you've been talking about. Securing OT networks is necessary but not sufficient. Compromising the process sensors can damage any process, yet neither the sensor comprised nor the system damaged may be identifiable by the OT networks.
>
> March 10, I gave a university seminar on the lack of cyber security in process sensors titled: "Shields Up and Good Cyber Hygiene Do Not Apply to Insecure Process Sensors". Process sensors have no inherent

cybersecurity but yet have direct connections to the Internet and 100 percent trusted input to OT networks. The cybersecurity gap includes no capability for passwords, single-factor (much less multi-factor) authentication, encryption, keys, signed certificates, etc. Moreover, process sensors have no cyber forensics.

Shields Up recommends conducting a test of manual controls to ensure that critical functions remain operable if the organization's network is unavailable or untrusted. Good cyber hygiene requires strong passwords. However, insecure process sensors have no passwords and are untrusted during all conditions. There have been more than 11 million control systems cyber incidents, many of them process sensor related, directly resulting in more than 1,500 deaths. The vast majority were not identified as being cyber-related, as there are no control systems cyber forensics at the process sensor layer. There's effectively no cybersecurity training for the control and safety systems engineers and technicians—even though cybersecurity training is available for the OT network personnel. Adversaries such as Russia, China, and Iran are aware of these deficiencies. It is not possible to be cyber secure, resilient, or safe if you cannot trust your process measurements.

There are a number of paths for moving forward. In the short term, get the engineers involved. I've heard nothing about that. Use sensor monitoring and analytics at the physics, not end word packet layer, to improve cybersecurity process safety product quality, resilience, and regulatory compliance. That cannot be done by monitoring the OT networks alone. Develop process sensor cyber forensics. Develop training recommendations and standards for process sensors. And in the long term, develop new cyber secure process sensors.

And with that, I really want to appreciate the ability to be able to provide these comments. Thank you.

Mr. Fanning thanked Mr. Weiss. Director Easterly asked Mr. Goldstein to weigh in on Mr. Weiss' remarks. Mr. Goldstein affirmed that industrial control systems (ICS) and OT security are foundational to CISA's mission and remains one of the Agency's top priorities. He stated that CISA needs to benefit from the extraordinary expertise in the research community, vendors, and asset operators to provide the best possible guidance and insights. He shared the example that the vulnerability and disclosure team released over 500 advisories last year on vulnerabilities in ICS and OT devices, each of which were the product of coordination between researchers, vendors, and owner-operators who deploy mitigations. Mr. Goldstein confirmed that CISA does work in collaboration with the engineers who develop the technologies deployed by CISA across ICS systems across the country. He also stressed CISA's goal to build and strengthen partnerships to address today's risks and threats and drive towards a future that is more secure and resilient by design, and process sensors are part of that equation. Mr. Goldstein closed by stating that ICS and OT security is one of CISA's top focus, CISA is working towards strengthening partners with experts across sectors to build a more secure technology ecosystem where control systems are more secure by design.

Closing Remarks and Adjournment

Director Easterly thanked the Committee members and other meeting participants for their subcommittee work and their input during the meeting. She identified trust and collaboration as key themes of the meeting and encouraged the subcommittees to work together to craft recommendations for CISA to share during the June CSAC Quarterly Meeting. Mr. Fanning and Mr. Green both provided brief closing remarks noting that the Committee's work matters and thanked members for their participation. Director Easterly adjourned the meeting.

APPENDIX: OPEN SESSION PARTICIPANT LIST

CSAC Members	Organization
Mr. Steve Adler	City of Austin, Texas
Ms. Marene Allison	Johnson & Johnson
Ms. Lori Beer	JPMorgan Chase
Mr. Robert Chesney	University of Texas
Mr. Thomas Fanning	Southern Company
Ms. Vijaya Gadde	Twitter
Dr. Patrick Gallagher	University of Pittsburgh
Mr. Ron Green	Mastercard
Ms. Niloofar Razi Howe	Tenable
Mr. Kevin Mandia	Mandiant
Mr. Jeff Moss	DEF CON Communications
Ms. Nuala O'Connor	Walmart
Ms. Nicole Perlroth	Cybersecurity Journalist
Mr. Ted Schlein	Kleiner Perkins Caufield & Byers
Mr. Stephen Schmidt	Amazon Web Services
Ms. Suzanne Spaulding	Center for Strategic and International Studies
Mr. Alex Stamos	Krebs Stamos Group
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
The Hon. Chris Inglis	NCD
Mr. Robert Costello	CISA
Ms. Alaina Clark	CISA
Mr. Chris DeRusha	Office of Management and Budget
Mr. Jonathan Dunn	CISA
Mr. Trent Frazier	CISA
Mr. Eric Goldstein	CISA
Ms. Mona Harrington	CISA
Ms. Rachel Liang	CISA
Mr. John (Jack) MacNeil	CISA
Ms. Celinda Moening	CISA
Mr. Nitin Natarajan	CISA
Mr. Barry Skidmore	CISA
Ms. Kiersten Todt	CISA
Ms. Megan Tsuyi	CISA

Ms. Kim Wyman	CISA

Contractor Support	Organization
Mr. Joseph Butler	TekSynap
Ms. Mariefred Evans	TekSynap
Ms. Marissa Pope	EdgeSource

Dial-In Participants	Organization
Ms. Mariam Baksh	NextGov
Mr. Mitchell Berger	Department of Health and Human Services
Mr. Christopher Bidwell	Airports Council International
Mr. Calvin Bieserker	Defense Daily
Ms. AmyClaire Brusch	Airports Council International
Mr. Jack Cable	Senate HSGAC
Ms. Sarahjane Call	Department of Homeland Security
Mr. Dan Callahan	Fortinet Federal
Ms. Anne Cutler	CISA
Ms. Jen DeBerge	Mastercard
Mr. Brett DeWitt	Mastercard
Ms. Victoria Dillon	CISA
Ms. Osasu Dorsey	Office of the National Cyber Director
Ms. Lisa Einstein	Stanford
Mr. Benjamin Flatgard	JPMorgan Chase
Ms. Amy Flowers	Microsoft
Mr. Christopher Frascella	Electronic Privacy Information Center
Ms. Sarah Friedman	Inside Cybersecurity
Mr. Will Garrity	Mastercard
Ms. Elizabeth Gauthier	CISA
Mr. Eric Geller	POLITICO
Ms. Michele Guido	Southern Company
Mr. Geoffrey Hale	CISA
Ms. Gwainevere Hess	CISA
Mr. Edward Humphrey	CISA
Ms. Helen Jackson	CISA
Mr. Matt Kehoe	Apple
Ms. Christina Lee	Beacon Global Strategies
Mr. Tom Leithauser	Telecommunications Reports and Cybersecurity Policy Report
Ms. Oumou Ly	CISA
Ms. Neysa Matthews	Walmart
Mr. Glenn Merell	Freelance Consulting
Mr. Mike Miron	Department of Homeland Security
Ms. Devi Nair	International Security Program
Mr. Phu Nguyen	Integrated Cybersecurity Engine

Mr. Andrew Nicholson	Imperium Global Advisors

Dial-In Participants	Organization
Ms. Maggie O'Connell	Interstate Natural Gas Association for America
Ms. Stacy O'Mara	Mandiant
Mr. Nick Ornstein	TwinLogic Strategies
Mr. Marty Reynolds	Airlines for America
Mr. Alexander Rodriguez	DP DHL Americas
Ms. Katheryn Rosen	JPMorgan Chase
Mr. Jason Sanford	Illinois Emergency Management Agency
Ms. Jordana Siegel	Amazon
Mr. Jordan Sims	Imperium Global Advisors
Mr. Tim Starks	CyberScoop
Mr. Travis Stoller	Wiley Law
Ms. Claire Teitelman	JPMorgan Chase
Mr. Wesley Trimble	Commonwealth Strategic Partners
Ms. Liz Turrell	CNN
Mr. Christian Vasquez	E&E News
Ms. Nicky Vogt	CISA
Mr. Joe Weiss	Applied Control Solutions, LLC
Ms. Erin Wieczorek	CISA
Mr. Ford Winslow	Integrated Cybersecurity Engine

CERTIFICATION

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

Tom Fanning (approved on 13 April 2022)

Mr. Tom Fanning
CISA Cybersecurity Advisory Committee Chair