# CISA CYBERSECURITY ADVISORY COMMITTEE
# SEPTEMBER 13, 2023 MEETING SUMMARY

## OPEN SESSION

### Call to Order and Opening Remarks

Ms. Megan Tsuyi, CISA, welcomed attendees to the Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Advisory Committee (CSAC) September Quarterly Meeting. She reviewed that while members of the public had the opportunity to provide public comments during the meeting, the Committee did not receive any requests to provide public comment. The Committee will accept comments at any time via the CSAC mailbox at CISA_cybersecurityadvisorycommittee@cisa.dhs.gov.

Mr. Tom Fanning, CSAC Chair, Southern Company, reflected on the impact of CSAC's contributions and explained that the main focus of the meeting was to discuss CSAC's recommendations to CISA. He thanked the CSAC members and CISA partners for their work. Mr. Ron Green, Mastercard, thanked all the Committee members for their contributions.

The Honorable Jen Easterly, CISA, thanked attendees and reviewed that the Committee would deliberate and vote on recommendations to CISA during the meeting.

### Subcommittee Updates / Deliberation and Vote

Mr. Fanning invited all subcommittee chairs to provide an overview of their actions to date and noted that draft recommendations were made available to all meeting participants and the public.

*Corporate Cyber Responsibility*

Mr. Dave DeWalt, NightDragon, provided an overview of the Corporate Cyber Responsibility (CCR) subcommittee's actions to date. He reviewed the recommendations to CISA to include: (1) CISA should work with relevant stakeholders to expand training programs; (2) CISA should identify what data is needed for engagement on cybersecurity, including a framework for effective board oversight; (3) CISA should create materials that explain risk for cybersecurity events, given that cyber breaches can have massive negative ramifications; and (4) CISA should sustain leadership and cooperation to create a culture of corporate cyber responsibility.

The Committee discussed concerns about the disparity in cybersecurity knowledge between board members of private companies and that of cybersecurity professionals. They discussed the Securities and Exchange Commission's (SEC) proposed rule from March 2022 that companies publicly declare one cybersecurity expert on the board of directors and one within management.

Mr. Fanning motioned that the Committee approve the recommendations. Committee members seconded and passed the motion.

*Turning the Corner on Cyber Hygiene*

Mr. George Stathakopoulos, Apple, provided an overview of the Turning the Corner on Cyber Hygiene (CH) subcommittee's actions to date. He reviewed the recommendations to include: (1) CISA should serve as an authoritative source of guidance for cybersecurity practices; 2) CISA should provide guidance for cybersecurity funding for organizations; and (3) CISA should provide expertise on how to implement best cybersecurity practices.

Committee members discussed CISA's actions over the past year regarding cybersecurity education for grades K-12, strong software practices, and protecting the nation, noting the need for further action.

Mr. Fanning motioned that the Committee approve the recommendations. Committee members seconded and passed the motion.

*National Cybersecurity Alert System*

Mr. Chris Inglis, Former Office of the National Cyber Director, provided an overview of the National Cybersecurity Alert System (NCAS) subcommittee's actions to date. He presented the recommendations to include: (1) CISA should proceed as the organization providing cybersecurity expertise; (2) CISA should work with stakeholders to better understand and identify respective outcomes; (3) implement those aforementioned outcomes as a federal framework, with CISA serving as the primary, but not sole, organization for cybersecurity information; (4) CISA should implement a tiered risk model; (5) CISA should build on the existing monitoring alert system and guidance processes; and (6) CISA General Counsel, in collaboration with other federal legal entities, should examine and recommend a legal framework, incentives, and protections connected to sharing and acting on cyber threat information.

Committee members discussed reconciling what rulemaking regulations come through the SEC with the National Cybersecurity Alert System. The group also discussed SEC notification requirements for the purpose of preventing inimical cybersecurity events.

Mr. Fanning motioned that the Committee approve the recommendations. Committee members seconded and passed the motion.

*Technical Advisory Council*

Mr. Jeff Moss, DEF CON Communications, reviewed the Technical Advisory Council (TAC) subcommittee's focus on supporting CISA's high-risk community protection (HRCP) program. CISA defines high-risk communities as meeting the following criteria: (1) demonstrated history of being targeted by advanced persistent threat (APT) actors; (2) limited capacity to provide for their own defense; and (3) limited cybersecurity assistance from the U.S. government. Mr. Moss reviewed the subcommittee's report to address the TAC scoping questions. He summarized the recommendations for CISA to partner with nonprofit organizations and non-government organizations performing security enhancement work in this space and amplify their work. He noted that CISA should prioritize the protection of life and minimize physical harm. He emphasized the serious need for high-risk communities to receive better guidance on how to mitigate threats. He noted CISA should prioritize developing and sharing information, resources, and tools to build on the successes of the Shields Up campaign.[1] The subcommittee acknowledged the significant gap of technical resources for communities to determine their risk and offered that CISA could provide threat modeling information to high-risk communities. To best support victims, the subcommittee upheld that the U.S. government could encourage secure-by-design requirements and promote collaboration to share threat intelligence. Ms. Nicole Wong, NWong Strategies, reflected that the Open Tech Fund advances similar work to protect high-risk communities.[2]

Mr. Fanning motioned that the Committee approve the recommendations. Committee members seconded and passed the motion.

*Transforming the Cyber Workforce*

Mr. Green emphasized that the Transforming the Cyber Workforce (TCW) subcommittee's focus to support CISA's efforts to recruit, develop, and retain top talent, and manage the remote and hybrid workforce. He reviewed the recommendation for CISA to gain access to Office of Personnel Management's annual employee survey data to include the Federal Employee Viewpoint Survey, and develop its own employee engagement survey. He suggested that CISA should create a focus group within the agency that includes the Chief People Officer and Chief Human Capital Officer and other key stakeholders within the agency.

[1] https://www.cisa.gov/shields-up
[2] https://www.opentech.fund/

Mr. Green reviewed three initiatives employed by the private sector from which CISA could benefit to include: (1) programmatic enhancements to include affinity groups; (2) cultural alignment efforts; and (3) formalizing and educating employees on growth and development. He noted that CISA should create greater opportunities for team members to share feedback on managers in addition to conducting exit interviews. To effectively manage a remote and hybrid workforce, CISA should develop a robust hybrid onboarding presentation, hold weekly welcome meetings, and convene teams in-person regularly to collaborate. Regarding internal mobility programs, he noted that CISA should implement an internal talent marketplace to identify career development opportunities, while also developing a tour of duty program. Lastly, he reflected that CISA should review its current approach to employee development to increase access to current and relevant trainings.

Mr. DeWalt suggested that CISA could leverage survey tools such as SurveyMonkey to empower staff to share feedback in an anonymous forum. Committee members upheld recommendations to leverage best practices from the private sector, but cautioned that CISA should not forget about the importance and uniqueness of their mission and culture. Director Easterly reflected on CISA's workforce and staffing accomplishments since the Committee's inception, to include hiring over 1,400 new employees. She upheld CISA's commitment to focusing on promoting its culture and mission, and removing bureaucratic hurdles when possible.

Mr. Fanning motioned that the Committee approve the recommendations. Committee members seconded and passed the motion.

*Building Resilience and Reducing Systemic Risk to Critical Infrastructure*

Mr. Fanning acknowledged that the subcommittee's tasking centered around ways both the private sector and the government can collaborate to improve the nation's security posture. He reviewed the group's action to create the architecture of collaboration across specific sectors. He encouraged CISA's National Risk Management Center to collaborate with the private sector as they advance work on the national risk register to evaluate the first, second, and third derivatives of risk across critical infrastructure. He noted that there is still work to be done to understand the criteria for systemically important entities (SIEs) and encouraged CISA to collaborate with the private sector to transparently advance this work.

Mr. Fanning reviewed the subcommittee's focus on defining the architecture of collaboration between the following sectors and government: energy, to include electricity, oil and natural gas, dams, and nuclear; finance; communications; transportation to include rail, airlines, shipping, and trucking; healthcare; and chemical. He reviewed the September 2022 recommendations and encouraged CISA to remain consistent with the Presidential Policy Directive-21 rewrite currently underway. As CISA starts to identify entities as systemically important, he encouraged CISA to evaluate the difference between Section 9 work and SIE designation and to obtain private sector support. This support should be forged through robust collaboration, and he noted that CISA's National Coordinator Role could help foster needed collaboration. He encouraged CISA to continue improving collaboration with private sector and sector risk management agency partners.

Committee members thanked Mr. Fanning for his leadership and lauded his focus on resiliency efforts. Mr. Fanning motioned that the Committee approve the recommendations. Committee members seconded and passed the motion.

## Closing Remarks

Director Easterly thanked the Committee for the valuable work to date. She thanked Chair Fanning for his support to the Committee. She also thanked Mr. Green and Mr. DeWalt for their future work as the new chair and vice chair. She asked that all subcommittees, other than SR and TAC, take a strategic pause while CISA responds to the recommendations. SR and TAC will continue advancing their taskings prior to the December Quarterly Meeting.

Mr. Fanning emphasized the value of the CSAC's work. Mr. Fanning and Mr. Green thanked Director Easterly for her leadership. Mr. Fanning adjourned the September CSAC Quarterly Meeting.

# APPENDIX: OPEN SESSION PARTICIPANT LIST

## CSAC Members

| Name | Organization |
|---|---|
| Steve Adler | Former Mayor of Austin, TX |
| Lori Beer | JPMorgan Chase |
| Dave DeWalt | NightDragon |
| Tom Fanning | Southern Company |
| Vijaya Gadde | Former Twitter |
| Brian Gragnolati | Atlantic Health System |
| Ron Green | Mastercard |
| Niloofar Razi Howe | Tenable |
| Chris Inglis | Former Office of the National Cyber Director |
| Rahul Jalali | Union Pacific |
| Jim Langevin | Former U.S. House of Representatives |
| Doug Levin | K12 SIX |
| Jeff Moss | DEF CON Communications |
| Nuala O'Connor | Walmart |
| Nicole Perlroth | Cybersecurity Reporter |
| Robert Scott | New Hampshire Department of Environment Services |
| Suzanne Spaulding | Center for Strategic and International Studies |
| George Stathakopoulos | Apple |
| Alicia Tate-Nadeau | Illinois Emergency Management Agency |
| Kevin Tierney | General Motors |
| Alex Tosheff | VMware |
| Nicole Wong | NWong Strategies |
| Chris Young | Microsoft |

## Government Participants

| Name | Organization |
|---|---|
| The Hon. Jen Easterly | CISA |
| Alaina Clark | CISA |
| Caitlin Conley | CISA |
| Jonathan Dunn | CISA |
| Lisa Einstein | CISA |
| Jamie Fleece | CISA |
| Elizabeth Gauthier | CISA |
| Eric Goldstein | CISA |
| Mona Harrington | CISA |
| Kirsten Heidelberg | CISA |
| Kathryn Coulter Mitchell | CISA |
| James Nash | CISA |
| Nitin Natarajan | CISA |
| Kiersten Todt | CISA |
| Megan Tsuyi | CISA |

## Contractor Support

| Name | Organization |
|---|---|
| James Eustice | Edgesource |
| Mariefred Evans | TekSynap |
| John Holland | TekSynap |
| Cedric Sharps | TekSynap |
| Xavier Stewart | Edgesource |

## Additional Attendees

| Name | Organization |
|---|---|
| Charles Abernathy | CISA |
| Ivy Bostock | CISA |
| Amy Claire Brusch | Airports Council International-North America |
| Brett DeWitt | Mastercard |
| Justin Doubleday | Federal News Network |
| Benjamin Flatgard | JPMorgan Chase |
| Sara Friedman | Inside Cyber Security |
| Eric Geller | The Messenger |
| Jonathan Grieg | The Record Media |
| Katherine Gronberg | NightDragon |
| Michele Guido | Southern Company |
| Bill Gulledge | American Chemistry |
| Joe Hamblin | Armis |
| Gwainevere Hess | CISA |
| Albert Kammler | Van Scoyoc Associates |
| Tom Leithauser | Cybersecurity Policy Report |
| Tomas Maldonado | National Football League |
| Avery Mulligan | CISA |
| Devi Nair | Center for Strategic and International Studies |
| Lily Pollard | CISA |
| John Sakellariadis | Politico |
| Brian Scott | Office of the National Cyber Director |
| David Strom | HotAir.com |
| Emily Trapani | House Appropriations Subcommittee on Homeland Security |
| Wesley Trimble | Commonwealth Strategic Partners |
| Christian Vasquez | CyberScoop |
| Joy Wangdi | LyondellBasell |

## CERTIFICATION

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

Mr. Tom Fanning (approved on 10 October 2023)
CISA Cybersecurity Advisory Committee Chair