CISA
CYBERSECURITY
ADVISORY
COMMITTEE

CISA CYBERSECURITY ADVISORY COMMITTEE
OCTOBER 11, 2024 MEETING SUMMARY

OPEN SESSION

Opening Remarks

The Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Advisory Committee (CSAC) Designated Federal Officer, Ms. Megan Tsuyi, CISA, welcomed attendees to the CSAC October Quarterly Meeting. 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@mail.cisa.dhs.gov.

The CSAC Chair, Mr. Ron Green, Mastercard, reflected on the Committee's work over the past two years. Mr. Dave DeWalt, CSAC Vice Chair, NightDragon, thanked the CSAC members and CISA partners for their work to date.

The Honorable Jen Easterly, CISA, underscored the importance of CISA's role as America's cyber defense agency and as national coordinator for critical infrastructure security and resilience. In the face of continued attacks on the nation's most sensitive critical infrastructure from China, an upcoming election, and environmental complications, she expressed her gratitude for the Committee.

Subcommittee Updates, Deliberation, and Vote

Mr. Green expressed his gratitude for the Committee members and invited all subcommittee chairs to provide an overview of their draft recommendations for full Committee deliberation and vote. He noted that draft recommendations were made available to all meeting participants and the public.

Building Resilience for Critical Infrastructure

Ms. Lori Beer, JPMorgan Chase, acknowledged that the Building Resilience for Critical Infrastructure (BR) subcommittee's tasking centered around ways CISA can best align its cybersecurity and resilience efforts to counter the actions of hostile actors towards the United States.

The BR subcommittee received briefings on current practices regarding cyber planning. Recent incidents have demonstrated that targeting of third-party vendors has the potential to expand damage wrought by cyber-attacks. As a result of the observations from meetings, the subcommittee developed the following draft recommendations for full Committee deliberation and vote: (1) CISA's Joint Cyber Defense Collaborative (JCDC) should work with Sector Risk Management Agencies to ensure resilience, contingency planning, and planning for nation-state conflict across all efforts for national critical infrastructure; (2) CISA's JCDC should enhance information sharing efforts, including risk mitigation and reliance; (3) CISA should increase the engagement of the vendor community and smaller Systemically Important Entities in cyber defense efforts; and (4) CISA should offer direct incentives and services to strengthen small vendors and help government efforts to collect targeted data. Ms. Beer thanked the subcommittee and staff for all their incredible work and active participation.

Committee members discussed how CISA can work with industry to amplify threat understanding, and how to collaborate to ensure long-term resilience. Collaboration has significantly improved over the years. CISA can continue to collaborate with industry via a shared dependence on third parties. The work that CISA is doing around Secure Our World, Secure by Demand, and Secure by Design will also enhance collaboration. The group also discussed the importance of working closely with CISA's JCDC to share their findings to further resilience. Committee members upheld that the country's infrastructure should be on a civil defense war framework. Dealing with cyber defense must be a long-term, systemic, inter-generational effort.

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

Secure by Design

Mr. George Stathakopoulos, Apple, provided an overview of the Secure by Design (SBD) subcommittee's actions to date. The group built on momentum of a previously developed secure by design whitepaper and continued to push companies to sign up for CISA's secure by design pledge. The group worked to evaluate how CISA could take a more active role in promoting this work, specifically to enhance the nation's critical infrastructure. The subcommittee found that private companies, by themselves, had little economic incentive to implement changes that would make their technology more secure by design. If no economic incentive exists, CISA should develop a cybersecurity impact study. The principle of secure by demand must come first from the private sector, and then government can work with the private sector on it. The public would also benefit from a guide to better understand which technologies are more secure by design than others.

The subcommittee developed the draft recommendations for full Committee deliberation and vote to position CISA to: (1) create a study, with clear metrics, to quantify the financial impacts and customer experience impacts of companies that have survived and recovered from a large-scale security event; (2) perform further studies to provide empirical data to substantiate whether fixing security vulnerabilities early in the software development lifecycle is truly more cost effective; and (3) take the first steps of a multi-year effort to secure critical infrastructure. The group discussed the importance of incentivizing private industry to create more transparency.

The group discussed the importance of transparency around the process. CISA does not want to create disincentives for the transparency and rapid disclosure from private industry.

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

Strategic Communications

Mr. DeWalt reviewed the draft Strategic Communications recommendations for full Committee deliberation and vote for CISA to: (1) increase CISA's strategic communications budget to meet growing demand; (2) develop key performance indicators for its strategic communications efforts and measure achievement of these; (3) incorporate communications strategies implemented by other U.S. agencies that have effectively cultivated stakeholder trust; (4) evaluate the technology platforms it uses to connect with stakeholder groups to identify new ways to connect with them; and (5) explore the use of additional technological capabilities to measure the effectiveness of CISA's strategic communications strategy and identify and counteract damaging counter narratives. Subcommittee discussed the importance of communication in a fractured communication environment.

Mr. Green 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 work to date and discussed the importance of Open-Source Software (OSS). He noted that the subcommittee discussed what version of OSS the public would utilize, the liability and legal regime around the software people consume, as well as the need for accountability by an intermediary.

Mr. Moss reviewed the draft recommendations for full Committee deliberation and vote to include: (1) CISA should produce a guidance document on Open-Source Consumption and Upstreaming. This guide would be used both as a technical guide for software engineers to understand the options around what to consider when selecting OSS components to use in their projects, as well as justification to management for upstreaming important changes that will benefit the source OSS project. (2) CISA should enhance existing awareness programs to promote OSS information sharing and norms, including the creation and maintenance of a clearing house with up-to-date information about OSS consumption, working to enhance the existing centralized curation services. CISA should investigate if the biggest improvements would come from centralizing and sharing accountability for safe consumption and keeping dependencies updated in one agency, perhaps in the style of the Department of Defense Iron Bank, but intended for all agencies, state, local, tribal and territorial governments, and critical sectors. (3) CISA should endorse the curation model for open source and encourage its use by federal agencies and their vendors to meet liability obligations and improve security in practice by shifting this burden to specialists. (4) CISA should emphasize the importance of “reproducible” builds and should extend that notion to encourage open source artificial intelligence (AI) models to enhance transparency, auditability and reproducibility including providing information on the model, the data, as well as the underlying data set.

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

Closing Remarks

Director Easterly thanked the Committee for their work to date to help ensure CISA is the agency the U.S. needs and can protect the country’s critical infrastructure. Mr. Green and Mr. DeWalt thanked the Committee, government partners, and attendees. Mr. Green adjourned the meeting.

APPENDIX: OPEN SESSION PARTICIPANT LIST

CSAC Members

Name	Organization
Lori Beer	JPMorgan Chase
Dave DeWalt	NightDragon
Brian Gragnolati	Atlantic Health System
Ron Green	Mastercard
Royal Hansen	Google
Rahul Jalali	Union Pacific
Jim Langevin	Former U.S. House of Representatives
Doug Levin	K12 Security Information eXchange (SIX)
Kevin Mandia	Google Cloud
Jeff Moss	DEF CON Communications
Robert Scott	New Hampshire Department of Environmental Services
Suzanne Spaulding	Center for Strategic and International Studies
George Stathakopoulos	Apple
Kevin Tierney	General Motors
Alex Tosheff	Former VMware
Nicole Wong	NWong Strategies

Government Participants

Name	Organization
The Hon. Jen Easterly	CISA
Michael Aycock	CISA
Robert Bacon	CISA
Bridget Bean	CISA
Caitlin Conley	CISA
Kathryn Coulter Mitchell	CISA
Trent Frazier	CISA
Jeff Greene	CISA
Helen Jackson	CISA
Bob Lord	CISA
Serita Morgan	CISA
James Nash	CISA
Nitin Natarajan	CISA
Jonathan Spring	CISA
Megan Tsuyi	CISA
Lily Wills	CISA
Lauren Zabierek	CISA

Contractor Support

Name	Organization
Jim Eustice	Edgesource
Mariefred Evans	TekSynap
John Holland	TekSynap
Xavier Stewart	Edgesource

Additional Attendees

Name	Organization
Moira Bergin	House Homeland Security Committee
Ashley Billings	CNN
AmyClaire Brusch	Airports Council International
Anne Disse	Apple
Justin Doubleday	Federal News Network
Benjamin Flatgard	JPMorgan Chase
Sara Friedman	Inside Cybersecurity
William Garrity	Mastercard
Eric Geller	Freelance reporter
Katherine Gronberg	NightDragon
Albert Kammler	Van Scoyoc Associates
Norma Krayem	Van Scoyoc Associates
Mike Miron	Department of Homeland Security
Robert Porter	Department of Interior
Aosheng Pusztaszeri	Center for Strategic and International Studies
Alexandra Seymour	House Homeland Security Committee
Charles Snyder	Google
Samuel Spector	Lenvo
Kendal Tigner	Senate Committee on Homeland Security Affairs and Governmental Affairs
Christian Vasquez	Cyber Scoop

CERTIFICATION

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

Mr. Ron Green (approved on 17 December 2024)
CISA Cybersecurity Advisory Committee Chair