CISA CYBERSECURITY ADVISORY COMMITTEE

CISA CYBERSECURITY ADVISORY COMMITTEE
JUNE 5, 2024 MEETING SUMMARY

OPEN SESSION

Call to Order and 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 June 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@cisa.dhs.gov.

The CSAC Chair, Mr. Ron Green, Mastercard, reflected on the Committee's work on the taskings from the Director and acknowledged the Director's work and her commitment to the success of the Committee. Mr. Dave DeWalt, CSAC Vice Chair, NightDragon, thanked the West Point staff, CSAC members, and CISA partners for their work to date.

The Honorable Jen Easterly, CISA, thanked the West Point staff for hosting the meeting. She thanked the Committee members for their partnership and advising on the work ahead.

Subcommittee Updates, Deliberation, and Vote

Optimizing CISA's Cyber Operational Collaboration Platform

Mr. Green summarized the subcommittee's findings and draft recommendations for full Committee deliberation and vote to examine CISA's Joint Cyber Defense Collaborative (JCDC) and focus on areas of collaboration and development. The draft recommendations are tailored to further mature JCDC's capabilities.

The findings encourage CISA to continue to amplify JCDC's focus on operational cyber defense. First, JCDC should continue and deepen its focus on operational collaboration and serve as a resource for those organizations involved in public policy. If this is successful, JCDC's day-to-day activities would center around operational collaboration, active incidents, or potential incidents. While JCDC and its members may be consulted on policy-centric questions, daily activities would not revolve around policy.

Second, CISA should clarify key operational components of JCDC, specifically, criteria for membership and participation in physical collaboration spaces. There is a strong desire for greater collaboration, even with stakeholders. Clarity and transparency around membership requirements and joining process would help to deepen JCDC's impact and value. JCDC should include elements of the federal agencies that engage in collaboration with the private sector to foster deeper coordination within the federal government. Further, there would be benefit in formalizing the structure and ongoing participation requirements for physical collaboration spaces. By bringing together the right entities for in-person collaboration, JCDC can deepen trust amongst participants and streamline the bi-directional sharing of actionable intelligence that is key for operational response. JCDC should develop new criteria for membership within 60 days. If this is successful, JCDC's purpose, function, and criteria for membership would be clear to not only current participants in JCDC but also to others interested in potentially becoming a member.

Third, CISA should leverage the convening power of JCDC to build out coordinating structures such as a proactive "smart rolodex" of public and private partners. A "smart rolodex" is a roster of the public and private sector members and their core competencies designed to make identifying potential partners simpler. CISA should connect these partners both proactively and reactively to improve collective defense capabilities. If this is successful, JCDC would have a clear process for identifying the appropriate partners for given situations and requests and an enhanced ability to respond to active issues.

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

Strategic Communications

Mr. DeWalt reviewed the subcommittee's actions to date to evaluate CISA's strategic communications efforts to amplify awareness of CISA's mission and to strengthen CISA's relationship with key stakeholders. Specifically, the subcommittee is considering how CISA can best encourage consumers to take action through the agency's messaging efforts. To inform the subcommittee's findings, the group has conducted briefings with communications professionals from other government agencies and industry partners.

Members discussed increasing CISA's budget for strategic communications and the importance of improving CISA's brand and how the agency articulates its value to the American people.

Building Resilience for Critical Infrastructure

Ms. Lori Beer, JPMorgan Chase, gave an overview of the subcommittee's actions to date. The subcommittee continues to examine how CISA can help critical infrastructure to build resilience for cyber-attacks in the face of strategic competition with nations that target American critical infrastructure. The subcommittee is examining (1) how the U.S. can enhance its defense against known tactics of hostile nation-state actors, and (2) how the U.S. can increase its resilience of critical state infrastructure in case of such attacks.

Committee members discussed increasing resilience within the water critical infrastructure sector, increasing information sharing and collaboration within the wider cyber ecosystem, and providing sector-specific guidance on CISA's cyber alerts.

Ms. Beer explained key themes of the subcommittee's findings such as tactics, techniques, and procedures; threat actors; information sharing challenges; critical infrastructure sector-specific insights; public-private sector collaboration; and supporting critical infrastructure sectors with less experience in cyber defense.

The group discussed the challenges of strategic collaboration across different sectors and public-private partnerships, including resource allocation, leveraging technical expertise, and supplying secure by design software products.

Technical Advisory Council

Mr. Royal Hansen, Google, discussed the Technical Advisory Council's tasking on researching how CISA can encourage migration toward open source software security. The subcommittee is examining 1) how CISA should encourage adoption of safe consumption norms and support fixes and enhancements of open source products, and (2) how CISA should shift the burden of maintaining secure by design products to commercialized companies. CISA has significant access to talent within the cybersecurity space to advance safe consumption. The group will focus on ways to link the obligations listed by curators to the visibilities of procurement organizations, with possibilities including automatic updates to a list of security requirements.

Director Easterly noted she would update the subcommittee's tasking to include the role artificial intelligence (AI) plays.

Secure by Design

Mr. George Stathakopoulos, Apple, reviewed the subcommittee's role in exploring opportunities to ensure secure by design best practices are affordable and accessible for all users. It is important that consumers start to demand products that are secure.

Director Easterly noted that she would update the subcommittee's tasking to include the role AI plays. AI tools benefit product defense when it comes to secure by design and secure coding. Also, vendors should dramatically decrease the number of exploitable flaws and defects. The Committee discussed the desired evolution from secure by design and towards secure by demand.

The Committee discussed factors of secure by design success, to include partners, edge devices, and incentives to which the public responds. The group highlighted the success of CISA's Known Exploited Vulnerabilities Catalog[1], how to incentivize private companies to publish their vulnerabilities, and the disparity of public demand for secure by design between sectors.

Closing Remarks

Director Easterly thanked the Committee for their work to date to make CISA the cyber defense agency the U.S. deserves. Mr. Green and Mr. DeWalt thanked the Committee, government partners, and attendees. Mr. Green adjourned the meeting.

[1] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Attendees

Committee Members

Name	Organization
Marene Allison	Former Johnson & Johnson
Lori Beer	JPMorgan Chase
Dave DeWalt	NightDragon
Brian Gragnolati	Atlantic Health System
Ron Green	Mastercard
Royal Hansen	Google
Chris Inglis	Former Office of the National Cyber Director
Rahul Jalali	Union Pacific
Jim Langevin	Former U.S. House of Representatives
Cathy Lanier	National Football League
Doug Levin	K12 Security Information eXchange (SIX)
Kevin Mandia	Google Cloud
Ciaran Martin	Former National Cyber Security Centre
Nicole Perlroth	Cybersecurity Reporter
Bob Scott	New Hampshire Department of Environmental Services
George Stathakopoulos	Apple
Kevin Tierney	General Motors
Alex Tosheff	Former VMware

Government Attendees

Name	Organization
The Hon. Jen Easterly	CISA
Alaina Clark	CISA
Caitlin Conley	CISA
Lisa Einstein	CISA
Jamie Fleece	CISA
Bob Lord	CISA
Serita Morgan	CISA
James Nash	CISA
Clayton Romans	CISA
William Rybczynski	CISA
Andrew Scott	CISA
Mohamed Telab	CISA
Megan Tsuyi	CISA
Erin Buechel Wieczorek	CISA
Lily Wills	CISA

Contract Support

Name	Organization
Mr. Jim Eustice	Edgesource
Ms. Mariefred Evans	TekSynap
Mr. John Holland	TekSynap
Mr. Cedric Sharps	Edgesource
Mr. Xavier Stewart	Edgesource

Additional Attendees

Name	
Sara Barker	CISA
Eric Bazail-Eimil	Politico
Bria Cousins	NBC Universal
Thomas B. Cross	ChannelPartner.tv
John Curran	Meritalk
Sunil Dadlani	Atlantic Health System
Justin Doubleday	Federal News Network
Ben Flatgard	JPMorgan Chase
Sara Friedman	Inside Cybersecurity
William Garrity	Mastercard
Eric Geller	Freelance Journalist
Deadra Ghostlaw	US Military Academy Board of Visitors
Jonathan Grieg	The Record
Katherine Gronberg	NightDragon
Bill Gulledge	American Chemistry Council
Rick Holmes	Union Pacific
Albert Kammler	Van Scoyoc Associates
Matt Kehoe	Apple
Norma Krayem	Van Scoyoc Associates
Thomas Leithauser	Cybersecurity Policy Report
Mike Miron	CISA
Stacey O'Mara	Mandiant
Erik Peterson	Crowdstrike
Paula Reynal	Center for Strategic and International Studies
John Sakellariadis	Politico
Marilyn Stackhouse	CISA
Claire Teitelman	JPMorgan Chase
Kendal Tigner	U.S. Senate Homeland Security & Governmental Affairs Committee
Ryan Toohey	Office of Jim Langevin
Glenn Thorpe	GreyNoise Intelligence
Christian Vasquez	CyberScoop
Angela Weinman	Former VMware
Terri Zimmerman	Cummins

CERTIFICATION

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

Mr. Ron Green (approved on 01 July 2024)
CISA Cybersecurity Advisory Committee Chair