

# CISA CYBERSECURITY ADVISORY COMMITTEE MARCH 21. 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 March 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 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, highlighted that CISA accepted or partially accepted the vast majority of recommendations approved by the Committee during the September 2023 meeting. She reviewed two key engagements of 2024 to include her testimony on CISA's work to counter the threats posed by the People's Republic of China and her trip to Ukraine. Director Easterly emphasized the need for continued U.S. support of Ukraine, as U.S. support is inextricably linked to the security of U.S. homeland, especially in cyberspace. U.S. failure to defend Ukraine is a failure to defend against China. Resilience efforts are essential, as CISA works by, with, and through partners to prepare Americans for potential attacks.

#### **Subcommittee Updates**

Mr. Green asked each subcommittee chair to deliver brief remarks on their subcommittee's actions to date.

#### Building Resilience for Critical Infrastructure

Ms. Lori Beer, JPMorgan Chase, noted the subcommittee would build on past recommendations regarding support to at-risk critical infrastructure sectors such as healthcare, and provide recommendations to help CISA build effective public-private partnerships to manage significant risks. The tasking examined cyber threats from nation-state actors to U.S. critical infrastructure to focus on increasing CISA's collaboration between government and critical infrastructure to detect and mitigate cyber threats. The group would also consider contingency scenarios to better prepare for future cyber-attacks.

#### Optimizing CISA's Cyber Operation Collaboration Platform

Mr. Green underscored the value of CISA's Joint Cyber Defense Collaborative (JCDC) from the start of the Russia and Ukraine conflict. Director Easterly is seeking recommendations on how CISA could optimize the JCDC and bolster collaboration with key partners. This would align with CISA's current efforts to review the JCDC's initial operating mandate and future visions. Key stakeholders including the financial services sector have provided feedback on the priorities for the platform. Mr. Eric Goldstein, CISA, highlighted the benefit in seeking the subcommittee's expertise. CISA is focused on building a model of voluntary operational collaboration that is frictionless, high trust, and outcome oriented. The Committee's recommendations will help CISA understand how to work with the right partners, ensure risk-based partnerships, and translate outcomes transparently for the public defenders. Committee members emphasized the importance of bringing public and private sectors together, as most critical infrastructure is owned by private sector.

#### Secure By Design

Mr. George Stathakopoulos, Apple, discussed the Committee's focus on enhancing CISA's cyber hygiene efforts, to include supporting CISA's work on a 2023 security by design paper, which was accepted by multiple countries. The group is focused on exploring reasons for organizations' resistance to security by design recommendations, along with costs and other factors. Mr. Doug Levin, K12 Security Information eXchange (SIX), expressed gratitude to CISA leadership for their collaboration and emphasized the importance of targeting the cyber-poor sectors. He questioned how CISA could identify organizations, specifically in the healthcare or water sectors, that are adopting secure-by-design principles.

#### Strategic Communications

Mr. DeWalt discussed ways CISA could refine and amplify communications for 2024, specifically concerning the Protect 2024 messaging around the upcoming elections. Mr. DeWalt emphasized the need to engage media, social media, and various constituents, including public and private organizations. The group will evaluate success in various sectors, including large corporations and government agencies.

#### Technical Advisory Council

Mr. Kevin Tierney, General Motors, briefed on behalf of the subcommittee chair, Mr. Jeff Moss, DEFCON Communications. The subcommittee is focused on helping CISA amplify adoption of memory safe languages and techniques to protect software through its design. The subcommittee is also focused on CISA's work promoting open-source software security. The group is tasked with exploring factors of open-source software, how companies use it, and how they are incentivized to use it safely and securely. The group will discuss how CISA can encourage users to leverage open-source mechanisms and evaluate the best ways of working with across various communities. Security should not be an added cost but should be built into a product's design.

## **Closing Remarks**

Director Easterly expressed appreciation for the work done over the course of the CSAC's lifespan and conveyed her excitement for the Committee's work ahead. Chair Green and Vice Chair DeWalt thanked attendees and underscored the importance of everyone's role in advancing cybersecurity. Chair Green adjourned the March CSAC Quarterly Meeting.

## **APPENDIX: OPEN SESSION PARTICIPANT LIST**

## **CSAC Members**

NameOrganizationLori BeerJPMorgan ChaseDave DeWaltNightDragonRon GreenMastercardNiloo Razi HoweTenableRahul JalaliUnion Pacific

Cathy Lanier National Football League

Doug Levin K12 Security Information eXchange (SIX)

Kevin Mandia Mandiant

Nicole Perlroth Cybersecurity Reporter

Suzanne Spaulding Center for Strategic and International Studies

George Stathakopoulos Apple

Kevin Tierney General Motors
Alex Tosheff Broadcom

Nicole Wong NWong Strategies

# **Government Participants**

Name Organization

The Hon. Jen Easterly CISA Alaina Clark **CISA** Caitlin Conley **CISA** Lisa Einstein CISA Jamie Fleece **CISA** Eric Goldstein **CISA** James Nash **CISA** William Rybczynski **CISA Andrew Scott CISA** Kiersten Todt CISA CISA Megan Tsuyi **Brandon Wales CISA** Lily Wills CISA

# **Contractor Support**

NameOrganizationJames EusticeEdgesourceMariefred EvansTekSynapJohn HollandTekSynapCedric SharpsTekSynapXavier StewartEdgesource

## **CISA CYBERSECURITY ADVISORY COMMITTEE**

# **Additional Attendees**

Name Organization

Sara Friedman Inside Cybersecurity
Eric Geller Freelance Reporter

Jonathan Grief The Record
Katherine Gronberg NightDragon

Sarah Jacob CISA Matt Kehoe Apple

Norma Krayem Van Scoyoc Associates
Tom Leithauser Cybersecurity Policy Report

Pouriya Mosadegh CISA Janelle Pace CISA

Kendal Polk Transportation Security Administration

Anne Riley CISA
John Sakellariadis Politico
Marilyn Stackhouse CISA

Jamie Tarabay Bloomberg

Kendal Tigner U.S. Senate Homeland Security & Governmental Affairs Committee

Catarina Tran Transportation Security Administration

Christian Vasquez Cyberscoop

Sean Wolridge CISA

# **CERTIFICATION**

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

Mr. Ron Green (approved on 22 APRIL 2024) CISA Cybersecurity Advisory Committee Chair