



CISA CYBERSECURITY ADVISORY COMMITTEE DECEMBER 10, 2021, MEETING SUMMARY

OPEN SESSION

Call to Order and Opening Remarks

Ms. Megan Tsuyi, Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Advisory Committee Designated Federal Officer, called the meeting to order. She provided a short summary of the *Federal Advisory Committee Act* rules governing the meeting and then turned the meeting over to the Honorable Jen Easterly, Director, CISA.

Director Easterly welcomed the attendees and introduced the Committee's new Chair, Mr. Tom Fanning, Southern Company, and Vice Chair, Mr. Ron Green, Mastercard. Mr. Fanning and Mr. Green then gave brief opening remarks. Mr. Fanning noted that it is both a moment of strategic risk and a moment of strategic opportunity for the United States and emphasized the need for the private sector and the government to work together to protect the Nation's interests. Mr. Ron Green added that the Committee creates an opportunity for a closer partnership between the private sector, industry, and academia.

Director Easterly then welcomed the Honorable John K. Tien, Deputy Secretary, Department of Homeland Security (DHS), to provide a keynote address.

Keynote Address

Deputy Secretary Tien applauded the diversity of viewpoints on the Committee and noted the importance of sharing wisdom, expertise, and insight from each area represented. He expressed his hope that the Committee will be able to help identify the gaps and vulnerabilities the United States currently faces and also provide solutions. He said that DHS is eager to hear the Committee's recommendations and that the members should challenge Director Easterly and all of DHS to take action on addressing the Nation's cybersecurity issues.

Director Easterly thanked Deputy Secretary Tien and introduced the Honorable Chris Inglis, National Cyber Director, to provide remarks.

Fortifying the Nation's Cybersecurity Posture

Director Inglis opened by stating that the United States needs to take the offensive in cyberspace and reframe what is believed to be possible and appropriate in terms of improving the resilience of the Nation's digital infrastructure. He added that, to address the current cyber threats, Government and industry need to do more than share information. He said that the Nation has an opportunity to develop a collective defense across Government, industry, and academia so that any attacker has to defeat the combined capabilities of all three adding that he is pleased with the work that CISA is doing in this regard. He charged the group to be proactive in showing that each member has something to add to the collaboration.

CISA's Big Challenges and Issues Tasking

Director Easterly stated that CISA has two important roles: 1) be the operational lead for federal cybersecurity; and 2) be the National Coordinator for Critical Infrastructure, Resilience and Security. She said that, of the two, she wants to focus on the critical infrastructure piece because the vast majority of critical infrastructure is

owned and operated by the private sector. To do this, she wants the Committee to provide input on how to move CISA from a focus on public-private partnerships to true operational collaboration.

Director Easterly noted that there are three efforts at CISA that she is particularly excited about. The first is the Joint Cyber Defense Collaborative (JCDC), which brings together the private sector along with the full power of Federal law enforcement, the Defense Department, and the Intelligence Community to address the cybersecurity threat in a proactive manner. The second effort is the CISA Cybersecurity Advisory Committee, which brings together strategic thinkers with a huge amount of expertise and experience and has the potential to magnify CISA's work collaboration and innovation and service to the nation. The third effort is the ongoing process of reshaping CISA's workforce through the Cyber Talent Management System.

Mr. Eric Goldstein, Assistant Director for Cybersecurity, CISA, discussed the need for greater visibility into the nation's critical infrastructure, noting that access to that information would allow CISA and other agencies to quickly develop actionable measures and actionable guidance that network defenders across the country can use to protect themselves before more intrusions occur. He emphasized that CISA cannot do this alone, and so the JCDC is building platforms where analysts from CISA as well as partners from Government and the private sector, potentially including cybersecurity companies, can work together to identify and collectively address threats across all of the networks they have visibility into.

Mr. Goldstein said that CISA plays a critical role in finding and fixing vulnerabilities, but that the only long-term solution is for the technology industry to adopt a more security-focused culture. He concluded by posing several questions to the Committee on how to address these issues: How can CISA shift the culture of technology more toward a security-focused model? How can CISA ensure that security features are easier to use and on by default? How can CISA and industry minimize the consequences of the use of technology in national critical functions?

Ms. Kiersten Todt, Chief of Staff, CISA, discussed CISA's efforts to build a strong cyber workforce, and how CISA can facilitate and drive that process. She noted that the agency is working to build relationships with non-traditional and underserved communities through partnerships with NPower, Girls Who Code, and the Cyber Warrior Foundation. Ms. Todt added that cyber is an interdisciplinary issue and the cyber workforce needs the skills of not just mathematicians, engineers and scientists, but also sociologists, psychologists, historians, politicians, and economists.

Director Easterly then turned to the first planned focus areas for the CISA Cybersecurity Advisory Committee: ***Transforming the Cyber Workforce***. She asked the members to provide their input. Ms. Lori Beer, JPMorgan Chase, said that employee retention is just as critical as creating a pipeline for entry level talent. She suggested that the Agency find a way to work with industry to provide corridors for employees to move back and forth between Government and industry. Ms. Nicole Wong, NWong Strategies, said two issues that stop candidates from working for the Government is its hierarchical nature and slow delivery process. She said this can frustrate cybersecurity specialists who are used to working with their company's leadership and moving fast to implement new ideas and solutions. Mr. Green said that MasterCard has a Cyber Talent Initiative that has MasterCard employees take positions in Government agencies for two-year terms to develop skills and knowledge that MasterCard cannot provide. He said this might be a model CISA could leverage. Mr. Ted Schlein, Kleiner Perkins Caufield & Byers, added that student loan relief would also be a big incentive to get candidates to join CISA and stay with the agency.

Director Easterly then moved to the topic ***Turning the Corner on Cyber Hygiene*** and asked Mr. George Stathakopoulos to give his thoughts. Mr. Stathakopoulos stated that it's almost impossible to ensure security across an entire supply chain as many small suppliers simply don't have the resources to address the issue. He said that, especially for small businesses, CISA needs to create a step-by-step guide to ensure these companies can provide at least the minimum level of security. Mr. Bobby Chesney, University of Texas, added that providing tax breaks to companies that work to improve cyber best-practices would also help. Ms. Suzanne Spaulding, Center for Strategic and International Studies, said that a long-term strategy would need to be education. Specifically, teaching civics so that children learn at a young age how their actions will impact others. Ms. Nicole Perlroth, Cybersecurity Journalist, added that using storytelling to explain how using multi-factor authentication

could have prevented major cyber-attacks could prove useful in this regard. Mr. Alex Stamos, Krebs Stamos Group, said that cloud providers should be required to include security features in their most basic sales packages. He noted that charging an additional fee to enable security creates a disincentive for customers to adopt these features. Mr. Green noted that mandates alone will not work, and that people need to be able to see the value of improving security. He suggested creating a cyber scorecard to grade companies on the cyber hygiene.

Director Easterly then asked Mr. Jeff Moss, DEF CON Communications, to discuss the topic of *Igniting the Hacker Community*. Mr. Moss said that internet problems are global problems and addressing them will require global participation and a community response. He added that CISA should work to redefine the language around cybersecurity to make it clear how mutually beneficial it is. Mr. Moss noted health language works really well: If you're fighting against cancer, you're not fighting only for America. You're fighting against a global problem. He said that kind of inclusive language would get a lot more traction from the academic community. He added that hackers and academics need to provide an easy means for Government and policymakers to talk to them and receive feedback. Ms. Perlroth added that action is also important. She said it's important for CISA to think about its initial partnerships and ask: "Can CISA partner with the civil society community? Can CISA's efforts primarily support human rights defenders?" Ms. Marene Allison, Johnson & Johnson, noted that the Food and Drug Administration's process for working with the research community by creating a means for an open dialogue might provide CISA a model. Mr. Chris DeRusha, U.S. Chief Information Security Officer, Office of Management and Budget, added that CISA should consider reaching out to small groups like the Cyber Civilian Corps. Ms. Easterly said she would create a Technical Advisory Council as a subcommittee to address these issues.

On the topic of *Protecting Critical Infrastructure from Misinformation & Disinformation*, Dr. Kate Starbird, University of Washington, noted that the level of disinformation being spread across information systems has been increasing dramatically in recent years. She noted that it was used in 2020 to undermine the U.S. election system and that it has also made it difficult for Governments to address crisis events like the COVID-19 pandemic. She said that the solution to addressing this is to teach people to care about whether what they're sharing is true or false. Mr. Chesney noted that it might be very difficult to get people to unlearn bad behavior like that as, after a while, it becomes an entrenched cognitive bias. He suggested that working with the various social media platforms to address the problem might be the best approach. Mr. Stamos and Ms. Allison noted that Government agencies are very bad at using their authority and platforms to push back against disinformation. Ms. Allison suggested that CISA create a playbook for agencies to use in responding to the spread of disinformation.

Director Easterly then turned to the topic of *Building Resilience & Reducing Systemic Risk to Critical Infrastructure*. Mr. Fanning stated that one of the biggest impediments to industry and Government working together to address systemic risk is identifying the truly critical elements in critical infrastructure. He said CISA can help develop solutions, but that industry will need to take the lead in working with the Government to address the problem. Mr. Fanning noted that there are a number of models that CISA and industry could build on, such as the Analysis and Resilience Center for Systemic Risk developed by the Finance and Energy sectors. He closed by stating that, because industry controls the vast majority of critical infrastructure in the United States, the end goal should be for the Government to provide industry the tools to defend themselves.

Director Easterly recommended the following subcommittee assignments:

- **Transforming the Cyber Workforce**
 - Mr. Green, Mastercard (Lead)
 - Ms. Lori Beer, JPMorgan Chase
 - Ms. Nicole Perlroth, Cybersecurity Journalist
 - Dr. Pat Gallagher, University of Pittsburgh
 - Ms. Nicole Wong, NWong Strategies
 - Ms. Kiersten Todt, CISA

- **Turning the Corner on Cyber Hygiene**
 - Mr. George Stathakopoulos, Apple (Lead)
 - Mr. Steve Schmidt, AWS
 - Ms. Chris Young, Microsoft
 - Mr. Alex Stamos, Krebs Stamos Group
 - Mr. Ted Schlein, Kleiner Perkins
 - Ms. Nuala O'Connor, Walmart
 - Mr. Eric Goldstein, CISA
- **Igniting the Hacker Community (Technical Advisory Council)**
 - Mr. Jeff Moss, DEF Con Communications (Lead)
 - Mr. Kevin Mandia, Mandiant
 - Ms. Wong
 - Mr. Goldstein
 - Mr. Chris DeRusha, NCD/OMB
- **Protecting Critical Infrastructure from Misinformation & Disinformation**
 - Dr. Kate Starbird, University of Washington (Lead)
 - Ms. Suzanne Spaulding, Center for Strategic & International Studies
 - Mr. Matthew Prince, Cloudflare
 - Ms. Alicia Tate-Nadeau, State of Illinois
 - Ms. Vijaya Gadde, Twitter
 - Ms. Kim Wyman, CISA
 - Mr. Geoff Hale, CISA
- **Building Resilience & Reducing Systemic Risk to Critical Infrastructure**
 - Mr. Fanning (Lead)
 - Ms. Marene Allison, Johnson & Johnson
 - Mr. Bobby Chesney, University of Texas
 - Ms. Beer
 - Mr. Bob Kolasky, CISA
- **Strategic Communications**
 - Ms. Howe, Tenable (Chair)
 - Mayor Steve Adler, City of Austin
 - Mr. Schlein
 - Ms. Perlroth
 - Ms. Jen Easterly, CISA
 - Ms. Todt

Public Comment Period

Mr. Patrick Gaul, National Technology Security Coalition, provided the following comment for the record:

Good afternoon. This is Patrick Gaul. And as the Executive Director of the National Technology Security Coalition or the NTSC, the organization that spearheaded the creation of the Advisory Committee, and very proud and excited to see it operational. I'm eager to see the Advisory Committee demonstrate its value to Director Easterly, CISA, and the nation. I'm also proud that NTSC board members Marene Allison and Ron Green, are members of the Advisory Committee. Marene and Ron are preeminent in the field and I know their contributions will be vital. I'd also like to congratulate JPMorgan Chase and Microsoft, for their membership on the Advisory Committee, as they both have a board presence with the NTSC as well. As the only national organization representing the Chief Information Security Officer or CISO, we are eager to make our voices heard. CISOs work hard every day on the front lines, to combat cyber threats and maintain our collective national security. I believe there's no one who understands

cybersecurity better than those that practice it every day and who are also in the front of implementing national policy and regulatory requirements. In most large companies today the CISO role has become a member of the C-suite and the member trusted to protect the interests of the company and the customers. We look forward to watching the committee engage the cyber challenges ahead of us. We also sincerely hope, as the committee expands, more CISOs will have an opportunity to serve. And of course, the NTSC stands ready to support the committee. Thank you for allowing me to speak.

Closing Remarks and Adjournment

Director Easterly thanked the Committee members and other meeting participants for their input during the meeting. She also thanked the CISA and MITRE teams for supporting the meeting. She then gave each member an opportunity to ask any final questions. The Committee's Chair, Mr. Fanning, and Vice Chair, Mr. Green, both provided closing remarks noting that the Committee was off to a great start and that they looked forward to working on the issues discussed during the meeting. Director Inglis also thanked the Director and the participants, adding that he believed the Committee can make a serious dent in addressing the Nation's cybersecurity threats. Director Easterly adjourned the meeting.

APPENDIX

OPEN SESSION PARTICIPANT LIST

CSAC Members

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
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

Organization**Government Participants**

The Hon. Jen Easterly	Cybersecurity and Infrastructure Security Agency (CISA)
The Hon. Chris Inglis	Office of the National Cyber Director (ONCD)
The Hon. John K. Tien	Department of Homeland Security (DHS)
Ms. Alaina Clark	CISA
Mr. Chris DeRusha	Office of Management and Budget
Ms. Osasu Dorsey	ONCD
Ms. Victoria Dillon	CISA
Mr. Jonathan Dunn	CISA
Mr. Eric Goldstein	CISA
Mr. Robert Kolasky	CISA
Mr. Brent Logan	CISA
Mr. Jason Mayer	DHS
Ms. Kaitlin Seale	CISA
Mr. Mark Stidd	CISA
Ms. Kiersten Todt	CISA
Ms. Megan Tsuyi	CISA
Ms. Kim Wyman	CISA

Organization

Other Attendees

Mr. Steve King

Contractor Support

Ms. Laura Karnas

Mr. Barry Skidmore

Ms. Quynh Tran

Ms. Jennifer Peters

Dial-In Participants

Mr. Payton Alexander

Mr. Lee Allen

Ms. Denise Anderson

Ms. Elizabeth Andrion

Mr. Billy Anglin

Ms. Felicia Archer

Ms. Mariam Baksh

Ms. Christina Berger

Mr. Musadiq Bidar

Mr. Christopher Bidwell

Mr. Calvin Biesecker

Ms. Ashley Billings

Mr. Charles Blackmore

Mr. Peter Bloniarz

Mr. Per Brekke

Ms. Cynthia Brumfield

Mr. Brandon Buchanan

Ms. Mary Byrd

Ms. Courtney Callejas

Ms. Genevieve Carnes

Mr. Christopher Castelli

Mr. Michael Chandaris

Ms. Alicia Chavy

Ms. Lodrina Cherne

Ms. Ruth Clemens

Mr. George Coleman

Ms. Kathryn Condello

Ms. Audrey Connors

Mr. Justin Cooksey

Ms. Bria Cousins

Ms. Ann Cutler

Ms. Jumoke Dada

Mr. Raymond Decerchio

Organization

MITRE

Organization

Booz Allen Hamilton

Insight

Insight

Nexight Group

Organization

Wiley Rein LLP

TSA

Health ISAC

Charter Communications

Sylint

TSA

Nextgov

CISA SED

CBS News

Airports Council International

Defense Daily

CNN

US Coast Guard

Office of Governor New York

Embassy of Norway

CSO Online

American Bus Association

TSA

US House of Representatives

Association of American Railroads

Booz Allen Hamilton

TSA

Beacon Global Strategies

Cybereason

CISA

TSA

Lumen

Charter Communications

Department of Energy

CNBC

CISA

R Street Institute

FAA

Dial-In Participants

Ms. Grace Dille
 Mr. Cameron Dixon
 Mr. Justin Doubleday
 Ms. Nzinga Dyson
 Mr. Obum Egolum
 Ms. Sharon Eshelman
 Ms. Katie Ewers
 Mr. Derrick Fail
 Ms. Michelle Feldstein
 Mr. Erik Fredrickson
 Ms. Sara Freidman
 Ms. Vijaya Gadde
 Mr. Rory Gallagher
 Mr. Michael Garcia
 Mr. Patrick Gaul
 Mr. Gregory Gavins
 Ms. Olivia Gazis
 Mr. Eric Geller
 Ms. Heather Gerard
 Ms. Leah Glaccum
 Ms. Tara Hairston
 Ms. Judith Harroun Lord
 Mr. Juan Hayes
 Ms. Katie Hazlett
 Mr. Andrew Hildick Smith
 Mr. Maurice Ed Hudson
 Mr. Michael Jacobs
 Mr. Eamon Javers
 Mr. Bob Joachim
 Mr. Lamar Johnson
 Mr. Derek Johnson
 Ms. Anne Johnson
 Ms. Jillian Joyce
 Mr. Albert Kammler
 Ms. Michealann Krause
 Ms. Norma Krayem
 Mr. Pradeep Kumar
 Mr. Jason Lamote
 Ms. Laura Laybourn
 Ms. Christina Lee
 Mr. Mark Lemmond

Organization

Meri Talk
 CISA
 Federal News Network
 Lewis Burke Associates LLC
 Capital One Financial
 Lewisburke Associates
 McKesson Corporation
 NOAA
 CISA OSPP
 Alaska Communications
 Inside Cybersecurity
 Twitter
 N/A
 Senate Homeland Security and Governmental Affairs
 National Technology Security Coalition
 Senate Homeland Security and Governmental Affairs
 CBS News
 POLITICO
 OASA ALT Army
 Defense Business Board
 Alliance for Automotive Innovation
 TSA
 TSA
 Commonwealth Strategic Partner
 Water ISAC
 CISA CSD
 TSA
 CNBC
 House Committee on Appropriations
 MeriTalk
 SC Media
 CISA CSD Contractor
 Committee on Homeland Security
 Van Scoyoc Associates
 Check Point Software Technologies
 Van Scoyoc Associates
 Tata Consultancy Services
 DHS Office of Legislative
 CISA NRMC
 Beacon Global Strategies
 US Department of Energy

Dial-In Participants

Mr. Harry Lesser
 Mr. Devin Lynch
 Mr. Rafi Martina
 Ms. Tina Martinez
 Mr. Scott McConnell
 Mr. George McElwee
 Mr. Tim McGiff
 Mr. Michael McWilliams
 Ms. Ceydi Mendoza
 Ms. Maggie Miller
 Ms. Celinda Moening
 Ms. Valerie Mongello
 Mr. Drew Morin
 Ms. Stacy O'Mara
 Mr. James Orgill
 Ms. Cheri Pascoe
 Ms. Andrea Peterson
 Ms. Nancy Pomerleau
 Mr. Matthew Prince
 Mr. Donald Andy Purdy
 Ms. Kayla Renner
 Mr. Chris Riotta
 Mr. Michael Rosado
 Mr. Chris Rose
 Mr. Edward Rothgery
 Mr. Michael Ryan
 Ms. Farida Salama
 Ms. Geneva Sands
 Mr. Fred Schwien
 Mr. Tony Sibert
 Mr. Eric Snyderman
 Ms. Janet St. John
 Ms. Donna Steward
 Mr. Peter Su
 Mr. David Sucherman
 Mr. James Tollerson
 Mr. Costis Toregas
 Mr. Wesley Trimble
 Ms. Kimberly Underwood
 Mr. Christian Vasquez
 Mr. Joe Viens

Organization

OASA ALT Army
 SecurityScorecard
 Senate Select Committee on Intelligence
 CISA SED
 CISA
 Commonwealth Strategic Partner
 Venable LLP
 Defense Innovation Board
 DHS TSA
 The Hill
 N/A
 CISA
 Tmobile
 Mandiant
 Identification Technology Part
 NIST
 The Record
 CISA SED
 Cloudflare
 Huawei Technologies USA
 Monument Advocacy
 FCW
 Syntelligen Analytic Solutions
 CISA
 NSA
 US Coast Guard
 TSA
 CNN
 Boeing
 CosmGroup LLC
 CISA CSD
 Assoc of American Railroads
 Hi Trust Alliance
 Senate Homeland Security and Governmental Affairs
 CNBC
 Norfolk Southern
 Montgomery County MD and GW U
 Commonwealth Strategic Partner
 AFCEA International
 E&E News
 Charter Communications

Dial-In Participants

Ms. Andrea Vittorio
Ms. Bridgette Walsh
Mr. Jonathan Walton
Mr. Michael Widomski
Mr. David Wood
Ms. Orlie Natalie Yaniv
Mr. Darnell Young
Ms. Bridget Zamperini

Organization

Bloomberg News
Financial Services ISAC
TSA
CISA
CISA
Gigamon
TSA
Federal Transit Administration

CERTIFICATION

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

Tom Fanning (approved on 18 December 2021)

Mr. Tom Fanning
CISA Cybersecurity Advisory Committee Chair