

2ND ANNUAL NATIONAL CYBERSECURITY SUMMIT

SEPTEMBER 18-20, 2019
GAYLORD AT NATIONAL HARBOR



CISA
CYBER+INFRASTRUCTURE

WEDNESDAY, SEPTEMBER 18, 2019; 12:30 PM - 4:30 PM

9:00 AM	<p style="text-align: center;"><u>Registration Opens</u> Lower Atrium</p>
12:30 PM – 4:30 PM	<p style="text-align: center;"><u>2nd Annual National Cybersecurity Summit Opening Kick-off</u> Riverview Ballroom</p> <p><i>Welcome and Opening Remarks</i> Christopher Krebs, Director, Cybersecurity and Infrastructure Security Agency</p> <p><i>Operationalizing a Collective Defense: Where Do We Go From Here?</i> Acting United States Deputy Secretary of Homeland Security, David Pekoske</p> <p><i>Transforming Government for the Cyber Age</i> Moderator: Jeanette Manfra, Assistant Director, Cybersecurity Division, Cybersecurity and Infrastructure Security Agency Panelists: <ul style="list-style-type: none"> • Anne Neuberger, Director, Cybersecurity Directorate, National Security Agency • Suzette Kent, Federal Chief Information Officer, Office of Management and Budget • Tonya Ugoretz, Deputy Assistant Director, Cybersecurity Division, Federal Bureau of Investigations • John (Jack) Wilmer, Deputy Chief Information Officer and Chief Information Security Officer, Department of Defense </p> <p><i>Cybersecurity and the Media</i> Moderator: Christopher Krebs, Director, Cybersecurity and Infrastructure Security Agency Panelists: <ul style="list-style-type: none"> • David Sanger, National Security Correspondent, New York Times • Alex Marquardt, Senior National Correspondent, CNN • Pam Fessler, Correspondent, National Desk, NPR • Chris Bing, Cybersecurity Reporter, Reuters </p> <p><i>Disinformation and How to Preserve Democracy</i> Clint Watts, Foreign Policy Research Institute</p> <p><i>National Cyber Strategy, One Year Later</i> Grant Schneider, Federal Chief Information Security Officer, Office of Management and Budget and Senior Director for Cybersecurity Policy, National Security Council</p>

THURSDAY, SEPTEMBER 19, 2019; 9:00 AM - 5:15 PM

8:00 AM	<p style="text-align: center;"><u>Registration Opens</u> Maryland Ballroom Registration Desk</p>
9:00 AM – 10:00 AM	<p style="text-align: center;"><u>2nd Annual National Cybersecurity Summit Day 2 Opening</u> Maryland Ballroom A&B</p> <p><i>Laying the Policy Groundwork for a Secure Tomorrow</i> Senator Mark Warner (D-VA)</p> <p><i>The Eagle's Eye: Strategic Perspectives from the C-Suite</i> Moderator: Michael Daniel, President and CEO, Cyber Threat Alliance Panelists: <ul style="list-style-type: none"> • Travis Reese, President, FireEye • Amit Yoran, Chairman and CEO, Tenable </p>

9:00 AM – 5:00 PM	<u>CISA EXPO – Educational demos, Capture the Flag and much more!</u> Maryland Ballroom C&D		
10:15 AM	Breakouts 1 - National Harbor Rooms	Protect 2020 (National Harbor 12 & 13)	<p>Building Trusted Relationships in the Cybersecurity Limelight; A #Protect2020 Primer</p> <p>Description: Hear from the front line as State election officials discuss working collectively with federal government and election infrastructure industry partners to protect the 2020 elections.</p> <p>Moderator: Ben Spear, Senior Intelligence Analyst, MS-ISAC</p> <p>Panelists:</p> <ul style="list-style-type: none"> • Chris Wlaschin, ES&S, Vice President Systems Security and CISO • Paul Pate, Secretary of State of Iowa • Keith Ingram, 24th District of Arkansas, Minority Leader • Donald Palmer, U.S. Election Assistance Commissioner • Matthew Masterson, Senior Cybersecurity Advisor, Cybersecurity and Infrastructure Security Agency
		Defend Today (National Harbor 3)	<p>Raising the Bar for Government Cyber: How Federal Initiatives and Binding Operational Directives are Helping Federal, State, and Local Governments Protect Citizen Data</p> <p>Description: Across all levels of government - federal, state, local, tribal and territorial - there has never been a more urgent need to protect the Nation's most critical systems and safeguard citizen data. This panel brings together State, city, and non-profit cybersecurity leaders to discuss the current state of cybersecurity across government entities, share tips and insights on mitigating emerging risks, and to outline how any organization can leverage government Cyber lessons learned and best practices to enhance their posture and implement cybersecurity at scale.</p> <p>Moderator: Mike Duffy, Deputy Associate Director, Cybersecurity Division, Cybersecurity and Infrastructure Security Agency</p> <p>Panelists:</p> <ul style="list-style-type: none"> • Geoff Brown, Chief Information Security Officer, New York City • John Evans, Chief Information Security Officer, State of Maryland • Philip Reitingger, CEO & President, Global Cyber Alliance
		Insights (National Harbor 10)	<p>Federal Cyber Leadership Perspectives</p> <p>Description: See what's top of mind for federal leaders, when it comes to cybersecurity. This session offers a glimpse into the challenges the Federal government faces in this area, and some of the approaches that those at the front of cybersecurity are taking.</p> <p>Moderator: Steven Hernandez, Chief Information Security Officer, Department Of Education</p> <p>Panelists:</p> <ul style="list-style-type: none"> • Grant Schneider, Federal Chief Information Security Officer, Office of Management and Budget • Jeanette Manfra, Assistant Director, Cybersecurity Division, Cybersecurity and Infrastructure Security Agency • Donna Dodson, Chief Cybersecurity Advisor, National Institute of Standards and Technology
		Partnerships in Action (National Harbor 11)	<p>Operational Collaboration: Moving Beyond Information Sharing</p> <p>Description: If you are regularly sharing information with public and private sector partners, you are off to a good start. However, security doesn't end there. Hear how industry and other leaders are moving beyond info-sharing and implementing actual operational collaboration.</p>

			<p>Moderator: David Forscey, Managing Director, Cyber and Technology Program, Aspen Institute</p> <p>Panelists:</p> <ul style="list-style-type: none"> • Michael Daniel, President and CEO, Cyber Threat Alliance • Niloofar Howe, Senior Operating Partner, Energy Impact • Chris Inglis, Managing Director, Paladin Capital Group
		Secure Tomorrow (National Harbor 2)	<p>Navigating the Now: 5G Security, Standards, and Deployment</p> <p>Description: Excitement and concern about 5G technology and its security abound, with the uncertainty of a new horizon generating discussion on many interconnected topics. Learn about four top-of-mind concerns for most industry specialists and cybersecurity practitioners as they unpack these issues and discuss the current state of play around 5G security.</p> <p>Moderator: Christopher Roberti, Senior Vice President, Cyber, Intelligence and Security Policy, US Chamber of Commerce</p> <p>Panelists:</p> <ul style="list-style-type: none"> • John Godfrey, Senior Vice President, Public Policy, Samsung • Jayne Stancavage, Executive Director, Communications Policy, Intel Corporation • Eric Wenger, Director for Government Affairs, Cisco • Michael J. Woods, Associate General Counsel, Verizon
11:15 AM	Network/Move to Breakouts		
11:30 AM	Breakouts 2 - National Harbor Rooms	Protect 2020 (National Harbor 12 & 13)	<p>Lifting the Fog of More: Finding (and Implementing) the Right Best Practices for Your Election</p> <p>Description: If your device is connected, it may be vulnerable. Hear from the experts at the Center for Internet Security about best practices and advice for internet connected devices and learn how you can use the Global Cyber Alliance's Election Toolkit.</p> <p>Panelists:</p> <ul style="list-style-type: none"> • Phil Reitingner, President and CEO, Global Cyber Alliance • Mike Garcia, Center for Internet Security • Aaron Wilson, Center for Internet Security
		Defend Today (National Harbor 3)	<p>Framing Public Safety Communications Cyber Risks: A Preview of the 2019 National Emergency Communications Plan & Strengthening Public Safety's Cybersecurity Posture</p> <p>Description: Rapid technological advancement and complex emergencies: these are two factors driving changes throughout public safety communications. Join this session to find out how public safety officials can strengthen their cybersecurity posture to ensure essential emergency communications functions like emergency 911, are there, when they are needed most.</p> <p>Moderator: Serena Reynolds, Policy Branch Chief, Emergency Communications Division, Cybersecurity and Infrastructure Security Agency</p> <p>Panelists:</p> <ul style="list-style-type: none"> • Todd Early, Assistant Chief, Infrastructure Operations, Texas Department of Public Safety • John Beltz, IT Security Manager, Public Safety Communications Research • George Perera, Captain, Miami-Dade Police Department

			<p>Is Privacy Possible? Privacy Considerations in Cybersecurity Policy</p> <p>Description: This panel will answer the question: How important is privacy? Is it a concern of the past, as some commentators have suggested, or is it still an important consideration on Capitol Hill, for Executive Branch policy-makers, and for corporate leaders? The panel will highlight a number of issues in the cybersecurity and emerging technologies space where privacy considerations need to be carefully addressed. Finally, the panel will also talk about examples of creating effective cybersecurity policies that protect privacy and civil liberties. .</p> <p>Moderator: Daniel Sutherland, Chief Counsel, Cybersecurity and Infrastructure Security Agency</p> <p>Panelists:</p> <ul style="list-style-type: none"> • Rosaline Cohen, Chief Counsel, Committee on Homeland Security, U.S. House of Representatives • James Burd, Acting Privacy Officer, Cybersecurity and Infrastructure Security Agency • Gregory Nojeim, Director of the Freedom, Security and Technology Project at the Center for Democracy & Technology • Craig Sharkey, Vice President and General Counsel of Walmart Technology and Digital Citizenship
		Partnerships in Action (National Harbor 11)	<p>Securing the Supply Chain through the ICT Supply Chain Partnership</p> <p>Description: Join CISA's Assistant Director for the National Risk Management Center (NRMC) Bob Kolasky and the other co-chairs of the Information and Communications Technology (ICT) Supply Chain Risk Management Task Force as they discuss the work being done by the Task Force to address risk associated with global supply chain and related third-party risk.</p> <p>Moderator: Daniel Kroese, Associate Director, National Risk Management Center, Cybersecurity and Infrastructure Security Agency</p> <p>Panelists:</p> <ul style="list-style-type: none"> • Bob Kolasky, Assistant Director, National Risk Management Center, Cybersecurity and Infrastructure Security Agency • Robert Mayer, Senior Vice President of Cybersecurity at USTelecom and Co-Chair of the Task Force • John Miller, Vice President of Policy and Senior Counsel at the Information Technology Industry Council and Co-Chair of the Task Force
		Secure Tomorrow (National Harbor 2)	<p>Emerging ICS Risk</p> <p>Description: The basis for this panel will explore new threats facing America's critical infrastructure. Many of today's buzzwords in ICS cybersecurity cross between sectors and/or don't fit clearly into a specific sector to address. These challenges include things such as 5G communications, diversified supply chain threats, and Industrial Internet of Things.</p> <p>Moderator: Jon Homer, Industrial Control Systems Specialist, Cybersecurity and Infrastructure Security Agency</p> <p>Panelists:</p> <ul style="list-style-type: none"> • Lesley Carhart, Principal Threat Hunter, Dragos • Bryson Bort, Founder and CEO SCYTHER

12:30 PM	<p><u>Lunch</u></p> <p>The hotel features many restaurants that are conveniently located, lunch is not provided by the conference.</p>		
1:30 PM	Breakouts 3 - National Harbor Rooms	Protect 2020 (National Harbor 12 & 13)	<p>Protecting States Against Ransomware Threats</p> <p>You hope this nightmare doesn't happen to your state or locality: all your computer files are held ransom by some unknown actor. The clock is ticking. Should you pay the ransom (and encourage more attacks)? Or do you hope for the best and try to access your files before they are corrupted or deleted forever? This session looks at this newer threat and provides advice and resources for preventing from happening to you.</p> <p>Moderator: Daniel Kroese, Associate Director, National Risk Management Center, Cybersecurity and Infrastructure Security Agency</p> <p>Panelists:</p> <ul style="list-style-type: none"> • Keith Ingram, Director of Elections, Texas • Ben Spear, Director, EI-ISAC • Don Benack, Acting Deputy Associate Director, Cybersecurity Division, Cybersecurity and Infrastructure Security Agency
		Defend Today (National Harbor 3)	<p>State Cyber Emergency Declarations</p> <p>Description: In a major cyber incident, how do you integrate outside assistance? Who leads a multi-organization response? And what changes will you make to prevent another incident? In this session, participants will hear from state leaders who have "been there." See how they applied emergency management principles to major cyber events and learn how they changed their approach to resilience and preparing for future attacks.</p> <p>Moderator: Jeff McLeod, Director, Homeland Security & Public Safety Division, National Governors Association</p> <p>Panelists:</p> <ul style="list-style-type: none"> • John Felker, Assistant Director, Integrated Operations Division, Cybersecurity and Infrastructure Security Agency • Kevin Klein, Director, Colorado Homeland Security Advisor • James Waskom, Director, Louisiana Office of Homeland Security and Emergency Preparedness
		Insights (National Harbor 10)	<p>Cyber Essentials</p> <p>Description: Just getting started with your cybersecurity program? Left out of the national cybersecurity conversation? Then this session is for you. Whether you are a small business, a local government, other community-based organization, you probably rely on internet connected tools and services to serve your population. That means you, too, are at risk of a cyberattack. Learn about CISA's work on a community-oriented plan to develop a set of cybersecurity practices that can add practical advice to help defend against threats like ransomware.</p> <p>Moderator: Moderator: Tony Sager, Senior Vice President and Chief Evangelist, Center for Internet Security</p> <p>Panelists:</p> <ul style="list-style-type: none"> • Bradford Willke, Assistant Director (Acting), Stakeholder Engagement Division, Cybersecurity and Infrastructure Security Agency • Abel Torres, Global Principal Policy Advisor, Underwriters Laboratories (UL) LLC • Ola Sage, Chief Executive Officer, CyberRx • Nicky Hudson, Director of Policy and Communications, UK National Cyber Security Centre (NCSC)

		<p>Partnerships in Action (National Harbor 11)</p>	<p>Preparing and Responding to Cyber Events: How Global Leaders in The Communications and IT Sectors Are Working Together to Protect the Digital Ecosystem</p> <p>Description: In the digital age, no entity is an island, to loosely paraphrase poet John Donne. A threat to one organization can become a threat to others. This session explores how global leaders in the communications and IT sectors have banded together to prepare themselves, the government, and the larger internet ecosystem to ward off cyber threats. Through the Council to Secure the Digital Economy (CSDE), 13 global companies have completed three operational work products to increase overall cyber resiliency and prepare for the worst. Learn how about these efforts and how you can leverage them to improve your own cyber risk posture.</p> <p>Moderator: Bob Kolasky, Assistant Director, National Risk Management Center, Cybersecurity and Infrastructure Security Agency</p> <p>Panelists:</p> <ul style="list-style-type: none"> • Jonathan Spalter, President and CEO, USTelecom • Niklas Heuvelodp, President and CEO, Ericsson North America • Claire Vishik, Intel Fellow, Corporate and Government Affairs, Senior Director, Trust Technology and Policy, Intel Corporation • Edna Conway, Chief Security Officer, Global Value Chain, CISCO • Craig Silliman, Executive Vice President and Chief Administrative, Legal, and Public Policy Officer, Verizon
		<p>Secure Tomorrow (National Harbor 2)</p>	<p>Software Assurance and Supply Chain: Making Quality and Security More Transparent</p> <p>Description: Security depends on secure software, yet currently, no detailed, measurable benchmark exists to assess the security of a software product or service. Some national and international standards describe specific attributes of software security (e.g., identity management), and NIST recently published a white paper providing high-level descriptions of secure development lifecycle practices. No existing benchmark, however, provides a detailed, holistic treatment of software security considerations, including relating to the processes of developing and maintaining software throughout its life cycle and to specific security capabilities of a product or service, that can help organizations describe and measure essential security outcomes. BSA, whose members develop some of the most widely used software in the world, has developed a software security framework, adopting the outcome-focused structure of the NIST critical infrastructure cybersecurity framework, for standardizing and assessing software security. The new framework is specific, detailed, and practically applicable across diverse types of software and software development processes. Moreover, as an outcome-focused approach, it avoids assessment approaches rooted in testing, which only capture security at a single point in the software life cycle. The framework is intended to provide developers, customers, and policymakers with a new tool to understand, assess, and ensure minimum security measures in software products and services.</p> <p>One key aspect of secure software is using third party components of good quality and security. A "software bill of materials" that lists third-party dependencies can help both software suppliers and enterprise customers understand what is in the products they build, ship, and use. In 2018, the National Telecommunications and Information Administration (NTIA) launched an open process that used experts across many sectors to identify challenges in assembling, sharing, and using these data. The second half of this talk will review the baseline approach to SBOM developed by stakeholders, and summarize the documented potential benefits to those who produce, acquire, and operate software across a range of industries.</p>

			<p>Panelists:</p> <ul style="list-style-type: none"> • Tommy Ross, BSA, Senior Director of Policy • Allan Friedman, Department of Commerce, National Telecommunications and Information Administration, Director of Cybersecurity
2:30 PM	Network/Move to Breakouts		
2:45 PM	Breakouts 4 - National Harbor Rooms	Protect 2020 (National Harbor 12 & 13)	<p>The State of Election Cybersecurity from the Front Lines: Hear from the State and Local Officials Charged with Protecting our Elections</p> <p>Description: Looking for good practices to secure elections in your state? Join this session to see what other States are planning and how they are working to secure the 2020 elections for their constituents.</p> <p>Moderator: David Becker, Center for Election Innovation and Research</p> <p>Panelists:</p> <ul style="list-style-type: none"> • Jocelyn Benson, Michigan Secretary of State • Frank LaRose, Ohio Secretary of State • Barb Byrum, Ingham County Michigan Clerk • Brian Corley, Pasco County FL Supervisor of Elections • Jeffrey Baez, CISO NY State Board of Elections
		Defend Today (National Harbor 3)	<p>The Threats Within: Identifying and Mitigating Insider Threats</p> <p>Description: Join Cybersecurity and Infrastructure Security Agency's Assistant Director for Infrastructure Security Brian Harrell as he moderates a discussion with industry leaders on insider threats to cyber and physical operations. This session will provide context on what insider threats are, how to identify indicators and mitigate potential insider threats, and what resources are available to help organizations in their own efforts.</p> <p>Moderator: Brian Harrell, Assistant Director, Infrastructure Security Division, Cybersecurity and Infrastructure Security Agency</p> <p>Panelists:</p> <ul style="list-style-type: none"> • Randall Trzeciak, Technical Manager, Enterprise Threat and Vulnerability Management Team, CERT, and Director, CERT Insider Threat Center at Carnegie Mellon University's Software Engineering Institute • Mark Weatherford, Global Information Security Strategist, Booking Holdings • Frank Cilluffo, Director, Auburn University's McCrary Institute for Cyber and Critical Infrastructure Security • Stan Partlow, Vice President and Chief Security Officer, AEP • Cathy Lanier, Chief Security Officer, NFL
		Insights (National Harbor 10)	<p>Six Years of Vulnerability Disclosure Policy in The Netherlands</p> <p>Description: Disclosing a vulnerability can make your organization feel...well... vulnerable. As we work to iron out good policies here in the U.S., see how another nation has implemented vulnerability disclosure policy, what they learned, and lessons for others who are working on this issue.</p> <p>Speaker: Dr. Jeroen van der Ham, Senior Researcher, National Cyber Security Centre (NCSC), Ministry of Justice and Security, and Assistant Professor of Computer Network Security, University of Twente</p>
		Partnerships in Action (National Harbor 11)	<p>Unifying Control System Efforts Across Government</p> <p>Description: As we deal with emerging risks, efforts may often start in separate pods, among different groups and at different levels. When it comes to industrial control systems, we need to think about how to unify</p>

			<p>efforts to ensure a consistent approach to securing critical infrastructure systems that are increasingly interconnected or interdependent with other infrastructure. Join senior government leader as they discuss current efforts in this area.</p> <p>Moderator: Bryson Bort, Founder and CEO SCYTHE</p> <p>Panelists:</p> <ul style="list-style-type: none"> • Jeanette Manfra, Assistant Director, Cybersecurity Division, Cybersecurity and Infrastructure Security Agency • Edwin Wilson, Deputy Assistant Secretary of Defense for Cyber Policy • Michael R. Dransfield, NSA Senior Technical Executive • Adrienne Lotto, Acting Principal Deputy Assistant Secretary for CESER, Dept of Energy
		Secure Tomorrow (National Harbor 2)	<p>National Critical Functions</p> <p>Description: The National Critical Functions (NCFs) apply a holistic risk management approach that focuses on better understanding the functions that an entity enables or to which it contributes, rather than focusing on a static sector-specific or asset world view. This session will explore the utility of National Critical Functions as a springboard for a wide range of risk management activities, such as capturing cross-cutting risks and dependencies.</p> <p>Moderator: Bob Kolasky, Assistant Director, National Risk Management Center, Cybersecurity and Infrastructure Security Agency</p> <p>Panelists:</p> <ul style="list-style-type: none"> • Norma Krayem, Senior Policy Advisor & Chair, Global Cybersecurity Privacy Policy and Regulatory Team, Holland & Knight • Ross Nodurft, Senior Director, Cybersecurity Services, Venable LLP • Kimberly Denbow, Senior Director, Security, Operations and Engineering Services, American Gas Association • Suzanne Spaulding, Senior Adviser, Homeland Security, CSIS
4:00 PM – 5:30 PM	<p align="center"><u>2nd Annual National Cybersecurity Summit Day 2 Closing</u> Maryland Ballroom A&B</p> <p><i>Taped Remarks:</i> Chairman Bennie Thompson (D-MS)</p> <p><i>Leading the Way: Developing Cybersecurity Policy That Can Adapt to Evolving Threats</i> Senator Ron Johnson (R-WI)</p> <p><i>Today's Military: Critical to a Collective Defense</i> United States Secretary of Defense, Mark Esper</p> <p><i>Own it, Secure it: A Call to Action For Everyone to Take an Ownership Role in Cybersecurity</i> Acting United States Secretary of Homeland Security, Kevin McAleenan</p>		
FRIDAY, SEPTEMBER 20, 2019; 9:00 AM - 12:45 PM			
8:00 AM	<p align="center"><u>Registration Opens</u> Maryland Ballroom Registration Desk</p>		
9:00 AM – 1:00 PM	<p align="center"><u>CISA EXPO – Educational demos, Capture the Flag and much more!</u> Maryland Ballroom C&D</p>		
9:00 AM – 1:00 PM	<p align="center"><u>CISA Job Fair</u> Maryland Ballroom A</p>		
9:00 AM	Breakouts 5 - National Harbor Rooms	Protect 2020 (National Harbor 12 & 13)	<p>What the Elections Industry is Doing to Secure the 2020 Elections</p> <p>Description: Behind the scenes, the vendor community is working to protect the 2020 elections. Learn how they are coordinating on vulnerability disclosure and other mitigation actions to ensure the integrity of the democratic process.</p>

			<p>Moderator: Peder Jungck, BAE Systems</p> <p>Panelists:</p> <ul style="list-style-type: none"> • Eric Coomer, Director of Product Strategy and Security, Dominion Voting Systems • Sam Derheimer, Director of Government Affairs, Hart InterCivic • Brian Hancock, Unisyn Voting • Chris Wlaschin, Vice President Systems Security and CISO, Election Systems and Software
	<p>Defend Today (National Harbor 3)</p>		<p>Executive Risk Dash Boarding: From Data Calls and GRC to ML-Based Cyber Risk Decision Making</p> <p>Description: Looking for a way to improve risk-based decision making in real time? Come see a demonstration of CISA's Continuous Diagnostics and Mitigation Program (CDM) Dashboard.</p> <p>Panelists:</p> <ul style="list-style-type: none"> • Judy Baltensperger, Project Manager, Continuous Diagnostics and Mitigation Program Management Office (CDM PMO), Cybersecurity and Infrastructure Security Agency • Dr. Garfield Jones, Deputy Project Manager, Continuous Diagnostics and Mitigation Program (CDM), Cybersecurity and Infrastructure Security Agency • Michael Zakrzewski, Director Cyber Technologies, ECS Federal • James Byroads, Lead Dashboard Developer, ECS Federal • Richard Im, Technology Partner, Elastic
	<p>Insights (National Harbor 10)</p>		<p>Congressional Perspectives – How to develop Cybersecurity Policy</p> <p>Description: Along with solid security practices in the private sector and in the public sector, well-considered laws are vital to the nation's efforts to fight online attacks and protect our critical infrastructure, intellectual property, and privacy. Join this session for a discussion among congressional staff who are working with their Members of Congress on this important issue.</p> <p>Moderator: Kirsten Duncan, Senior Advisor, Cybersecurity and Infrastructure Security Agency</p> <p>Panelists:</p> <ul style="list-style-type: none"> • Moira Bergin, CHS Majority • Sarah Moxley, CHS Minority • Mike Flynn, HSGAC Majority • Jeff Rothblum, HSGAC Minority • Bob Joachim, HAC Majority
	<p>Partnerships in Action (National Harbor 11)</p>		<p>The Importance of Vulnerability Handling – A Discussion with the Cybersecurity Tech Accord</p> <p>Description: Good security requires well-informed policies on vulnerability handling and disclosure for both governments and the private sector. During this panel, representatives from across the technology industry will discuss the nuances of this important topic, including different approaches to vulnerability handling in different contexts and thoughts on the current regulatory environment and what would help to further improve security.</p> <p>Moderator: Gregory T. Nojeim, Senior Counsel & Director of Freedom, Security and Technology Project</p> <p>Panelists:</p> <ul style="list-style-type: none"> • Amanda Craig, Director, Cybersecurity Policy, Microsoft • Ed Cabrera, Chief Cybersecurity Officer, Trend Micro

			<ul style="list-style-type: none"> • Alex Bauert, Senior Director Threat Research Center, ThreatModeler • Vince Jesaitis, Director, Government Affairs, Arm
		Secure Tomorrow (National Harbor 2)	<p>Identifying and Managing Emerging Risks</p> <p>Description: Technology is evolving at a historically unprecedented pace and society is more technologically dependent than ever before. Emerging technologies present the opportunity for societal benefit, mission enhancement, and cost savings and efficiencies. However, these technologies may also present risks from unintended consequences, adversarial use, or accidents.</p> <p>Moderator: Mary McGinley, Physical and Cyber Security Portfolio Director DHS S&T</p> <p>Panelists:</p> <ul style="list-style-type: none"> • Christina I. Ray, Senior Managing Director for Market Intelligence, Omnis • Mark P. Harvey, Special Assistant to the President and Senior Director for Resilience Policy, National Security Council • Bryan Ware, Assistant Secretary Cyber, Infrastructure and Resilience Policy, Department of Homeland Security
9:45 AM	Network/Move to Breakouts		
10:00 AM	Breakouts 6 - National Harbor Rooms	Protect 2020 (National Harbor 12 & 13)	<p>Learning from Global Partners: Election Tampering at Home & Abroad</p> <p>Description: Since Russia meddled in the 2016 U.S. Presidential election, the cyber security community has gone into overdrive to determine how we can strengthen our defenses against foreign interference. In this session, we will see how public, private partnerships, technology and innovation all contribute to a collective defense. Panelists will analyze several elections from the past two years, including the Cambodian Elections in 2018, Israeli, Taiwan and Ukrainian elections.</p> <p>Speaker: Katelyn Marie Bailey, Program Manager, Strategic Intelligence and Government Team, FireEye, Inc</p>
		Defend Today (National Harbor 3)	<p>Cybersecurity: The States are Stepping Up</p> <p>Description: At the intersection of cybersecurity and emergency management, there are a set of similar requirements: coordination, shared situational awareness, communications, and escalation procedures and processes. Learn how states are applying all-hazards planning and operations models to cybersecurity. Panelists will share State efforts to apply emergency management principles to the substance of cyber security issues –threat vector, attack surface, and consequence– to achieve resilience.</p> <p>Moderator: Bradford Willke, Assistant Director (Acting), Stakeholder Engagement Division, Cybersecurity and Infrastructure Security Agency</p> <p>Panelists:</p> <ul style="list-style-type: none"> • Jared Maples, Homeland Security Advisor, State of New Jersey • Erik Avakian, CISO, Commonwealth of Pennsylvania • Shawn G. Talmadge, Assistant Secretary of Public Safety and Homeland Security, Commonwealth of Virginia
		Insights (National Harbor 10)	<p>Effective Cyber Risk Oversight for Corporate Boards</p> <p>Description: Boards of Directors and senior management have complimentary, but distinctively different, roles and responsibilities in cybersecurity. Learn about five key principles for Board oversight, as well as a series of “tool-kits” to assist boards in addressing key cyber issues with senior management.</p>

			<p>Panelists:</p> <ul style="list-style-type: none"> • Larry Clinton, Internet Security Alliance, President National Association of Corporate Directors • Daniel Kroese, Associate Director, National Risk Management Center • Peter Gleason, President/CEO, National Association of Corporate Directors
		Partnerships in Action (National Harbor 11)	<p>Smart Secure Cities and Communities</p> <p>Description: Working on a smart city? The “Smart Secure Cities and Communities Challenge (SC3),” sponsored by NIST and DHS, has helped more than 200 cities build cybersecurity and privacy in their smart city initiatives from the start. Come learn about good practices, including privacy, early adoption use cases and capacity building resources.</p> <p>Moderator: Lan Jenson, CEO, Adaptable Security Corp</p> <p>Panelists:</p> <ul style="list-style-type: none"> • Scott Tousley, Senior Executive of Cyber Program, Splunk • Christos Papadopoulos, Program Manager, DHS Science & Technology • Lee McKnight, Associate Professor, School of Information Studies, Syracuse University • James Burd, Acting Director, Privacy, Cybersecurity and Infrastructure Security Agency
		Secure Tomorrow (National Harbor 2)	<p>Innovation in Federal Cloud Security</p> <p>Description: The cloud has enabled a dramatic digital transformation across the public and private sectors. Hear perspectives from key members of the security ecosystem—cybersecurity, cloud service, and managed service providers— as they look at unique challenges and opportunities in this space. See how they address the challenges through a shared security model and learn why integrated partnerships are critical to holistically ensuring infrastructure and data security in cloud environments.</p> <p>Moderator: John F. Banghart, Senior Director for Technology Risk Management, Venable, LLP</p> <p>Panelists:</p> <ul style="list-style-type: none"> • John Morello, Vice President, Product Management, Palo Alto Networks • Mark Ryland, Director, Office of the Chief Information Security Officer, Amazon Web Services • Karina Homme, Senior Director, Azure Government, Microsoft • Shaan Mulchandani, Senior Manager, Accenture Security • Robert Ames, VMware Senior Director National Technology Strategy
10:45 AM	Network/Move to Breakouts		
11:00 AM	Breakouts 7 - National Harbor Rooms	Protect 2020 (National Harbor 12 & 13)	<p>Disinformation Panel: Building Resilience in the American Public</p> <p>Description: Do you know how to identify a disinformation campaign? Join CISA’s senior cybersecurity advisor and a panel of experts to learn about this threat to the electorate and the steps government and industry are taking to raise the public’s awareness of the threats.</p> <p>Moderator: Matthew Masterson, Senior Cybersecurity Advisor, Cybersecurity and Infrastructure Security Agency</p> <p>Panelists:</p> <ul style="list-style-type: none"> • Mac Warner, West Virginia Secretary of State • Laura Rosenberger, Director of the Alliance for Securing Democracy • Nathaniel Gleicher, Head of Cybersecurity Policy Facebook

		<p>Defend Today (National Harbor 3)</p>	<p>We Have an Emergency: Cyber Risks to our Nation’s 911 System</p> <p>Description: What do you do when 911 doesn’t work? Hear from National 911 Office and public safety subject matter experts about risks to the nation’s 911 networks and learn what leaders in the 911 community are doing to plan for and mitigate cyber incidents today, as well as cybersecurity concepts being refined for tomorrow’s 911 community.</p> <p>Moderator: Gerald (Jerry) Jaskulski, Emergency Communications Division, Cybersecurity and Infrastructure Security Agency</p> <p>Panelists:</p> <ul style="list-style-type: none"> • Laurie Flaherty, Coordinator, Department of Transportation, National 911 Program • Steve Verbil, State Emergency Telecommunications Manager, Connecticut • Tyrell Morris, Executive Director, Orleans Parish Communication District
		<p>Insights (National Harbor 10)</p>	<p>Legal, Policy and Operational Developments in Supply Chain Security</p> <p>Description: As our world becomes dramatically more connected to the Internet over the next decade, we will need to have governance, frameworks and laws that ensure new technologies are deployed in ways that protect our security and liberties—up and down the supply chain. Learn how 5G, the Internet of Things, “smart cities,” and other technologies can impact supply chain security, along with legal and policy frameworks that have developed to address these and other supply chain issues.</p> <p>Moderator: Daniel Sutherland, Chief Counsel, Cybersecurity and Infrastructure Security Agency</p> <p>Panelists:</p> <ul style="list-style-type: none"> • Gabriel Slater, Cybersecurity and Infrastructure Security Agency, Senior Counsel – Cybersecurity • Joyce Corell, Supply Chain and Cyber Directorate National Counterintelligence and Security Center, Assistant Director • Daniel Kroese, Associate Director, National Risk Management Center, Cybersecurity and Infrastructure Security Agency • Edna Conway, CISCO, Chief Security Officer, Global Value Chain
		<p>Partnerships in Action (National Harbor 11)</p>	<p>Cyber-Physical Convergence</p> <p>Description: Tackling some of our nation’s most difficult and complex security threats requires a collaborative and holistic approach. Join industry and thought leaders as they convene a fireside chat on the converging cyber and physical worlds, what it means from a security stance, and what we are doing about it.</p> <p>Moderator: Brian Harrell, Assistant Director, Infrastructure Security Division,, Cybersecurity and Infrastructure Security Agency</p> <p>Panelists:</p> <ul style="list-style-type: none"> • Dr. Paul Stockton, Managing Director of Sonecon LLC, an economic and security advisory firm in Washington, DC • Bill Lawrence, Vice President and Chief Security Officer for the North American Electric Reliability Corporation (NERC) • Scott Aaronson, Vice President for Security and Preparedness, the Edison Electric Institute • Mark Herrerra, Director of Education and Life Safety for the International Association of Venue Managers

		Secure Tomorrow (National Harbor 2)	<p>Leveraging Data in a Big Way</p> <p>Description: If cyber & risk is the fight, data is the logistics that enables our force. CISA's CTO will lead a panel how to leverage the power of data. Leaders in data management, engineering, and research will discuss the approaches to optimize use of this strategic asset.</p> <p>Moderator: Brian Gattoni, Chief Technology Officer, Cybersecurity and Infrastructure Security Agency</p> <p>Panelists:</p> <ul style="list-style-type: none"> • Preston Wertz, Chief Data Officer, Cybersecurity and Infrastructure Security Agency • Martin Gross, Associate Director, Cybersecurity Division, Cybersecurity and Infrastructure Security Agency • Beth Magen, Johns Hopkins University Applied Physics Laboratory • Aaron Mannes, Senior Policy Advisor, Science & Technology Directorate, Department of Homeland Security
11:45 AM	Network/Move to Breakouts		
12:00 PM	Breakouts 8 - National Harbor Rooms	Protect 2020 (National Harbor 12 & 13)	<p>Election Security Panel – “Working to protect digital democracy”</p> <p>Description: In this fireside chat, come hear how Microsoft approaches the task of defending democratic institutions. Senior Director of Microsoft's Defending Democracy Program, Jan Neutze, will discuss how they are working with political campaigns, private sector election providers, the U.S. Election Assistance Commission, and state and local officials on issues from disinformation campaigns to securing voting machines for the 2020 elections.</p> <p>Moderator: Matthew Masterson, Senior Cybersecurity Advisor, Cybersecurity and Infrastructure Security Agency</p> <p>Speaker: Jan Neutze, Sr. Director of Microsoft's Defending Democracy Program</p>
		Defend Today (National Harbor 3)	HOLD
		Insights (National Harbor 10)	<p>The Carrot and the Stick: Regulatory and Enforcement Approaches to Cybersecurity</p> <p>Description: Is voluntary collaboration enough to ensure cybersecurity? In a perfect world, maybe. But in reality, it may take both incentives and mandates to make sure we get where we need to be on the cybersecurity front. Join a discussion the merits and potential drawback of implementing regulations and enforcement to promote the level of cybersecurity we need for national and economic security.</p> <p>Moderator: Daniel Sutherland, Chief Counsel, Cybersecurity and Infrastructure Security Agency</p> <p>Panelists:</p> <ul style="list-style-type: none"> • Jim Trilling, Federal Trade Commission • Patti Adair, Consumer Product Safety Commission • Cheri Falvey, Crowell & Moring
		Partnerships in Action (National Harbor 11)	<p>Collaborative Security - The Role of Information Sharing in Protecting Critical Infrastructure</p> <p>Description: Hear from the experts about ways to share information across the critical infrastructure sectors, as well as the challenges they face and the benefits of sharing, including during incident response.</p>

		<p>Moderator: Andy Jabbour, co-founder and Managing Director of The Gate 15 Company and the Faith-Based Information Sharing & Analysis Organization (FB-ISAO)</p> <p>Panelists:</p> <ul style="list-style-type: none"> • Josh Poster, Automotive ISAC • Scott Algeier, IT ISAC • Carlos Kizzee, Retail and Hospitality ISAC • Joe Viens, Senior Director, Government Affairs, Charter Communications Inc.
	Secure Tomorrow (National Harbor 2)	<p>Working to Own IT. Secure IT. Protect IT. - Workshop</p> <p>Each and every one of us needs to do our part to make sure that our online lives are kept safe and secure. Learn what you can do to participate in National Cybersecurity Awareness Month this October and what steps can be taken to ensure your security while online.</p>
1:00 PM	Summit Concludes	



CISA
CYBER+INFRASTRUCTURE

