National Summit on State Cybersecurity

Shreveport-Bossier, Louisiana
Shreveport Convention Center
Ballroom A/B, Level 2
May 14-15, 2019

Monday, May 13, 2019 – Arrival & Check-In	
1:00 – 7:00pm *Pre-Function Area Ballroom A/B*	**Registration**
6:00 – 7:00pm	**Welcome Drinks**

Tuesday, May 14, 2019	
7:30 – 8:15am *Pre-Function Area Ballroom A/B*	**Registration and Breakfast**
8:15 – 8:45am *Ballroom A/B*	**Color Guard, Welcome Remarks & Agenda Overview** - **Jeff McLeod**, Director, Homeland Security & Public Safety, National Governors Association - **Major General Glenn H. Curtis**, Adjutant General, Louisiana National Guard
8:45 – 9:30am *Ballroom A/B*	**Preparing the Grid for a Dark Sky Event** *Several books, movies, and media speculate on electrical grids' ability to withstand cyber attacks. Less talked about is how states and private sector partners are collaborating to prevent a dark sky scenario. This session brings together these voices to discuss how they are preparing to defend the grid against cyber attacks.* - **Jeff McLeod**, Director, Homeland Security & Public Safety, National Governors Association (Moderator) - **Nick Akins**, Chief Executive Officer, American Electric Power - **Sharon Chand**, Principal, Cyber Risk Services, Deloitte - **Major General Donald Dunbar**, Adjutant General, Wisconsin
9:30 – 10:30am *Ballroom A/B*	**Cybersecurity and The Whole-of-State Approach** *Governors confronting the challenges associated with cybersecurity must foster collaboration among state agencies, localities, the private sector, and more. In this session, state participants will learn how they can employ a whole-of-state approach to help confront cyber threats that implicate health and safety from a cross-sector of essential disciplines necessary for a coordinated cybersecurity approach.* *Speakers:* - **Doug Robinson**, Executive Director, National Association of State Chief Information Officers (Moderator)

	- **Eric Boyette**, State Chief Information Officer, North Carolina - **Major General Glenn H. Curtis**, Adjutant General, Louisiana National Guard - **Jared Maples**, Director, Office of Homeland Security & Preparedness, New Jersey - **Mike Watson**, State Chief Information Security Officer, Virginia
10:30 – 10:45am	**Break**
10:45 – 11:15am *Ballroom A/B*	**Cybersecurity & Crisis Communications** *Security failures are inevitable, and in today's media environment they quickly attract public attention. Learn how to prepare for and manage public communications during and after a cyber incident.* **Speaker:** - **Siobhan Gorman**, Partner, Brunswick Group
11:15 – 12:00pm *Ballroom A/B*	**Lightning Talks** **Hard Truths: Artificial Intelligence & Cybersecurity** *Artificial intelligence has the promise to dramatically change every facet of life and cybersecurity itself is not immune from disruption. This talk will discuss how AI is not a panacea for cybersecurity and how human operators are still essential for the future of cybersecurity.* - **Dimitri McKay**, Security Architect and Evangelist, Splunk **Views from Abroad: The Israeli Cybersecurity Approach** *Israel is viewed as a premier leader in cybersecurity technology, entrepreneurship, and defense. Hear how Israel created this environment and applicable strategies relevant for state officials.* - **Hudi Zack**, Chief Executive Director, Technology Unit, Israel National Cyber Directorate
12:00 – 12:30pm *Ballroom C/D*	**Break and Lunch (Sponsored by Raytheon)**
12:30 – 1:00pm *Ballroom A/B*	**Lunch Session: Supply Chain Resilience** Over the past few years, the cybersecurity community has underscored the essential challenges associated with assessing risks to the supply chain. This talk will detail how we can mitigate the risk posed downstream through the supply chain. *Speaker:* - **Jon Check**, Senior Director, Cyber Protection Solutions, Cybersecurity and Special Missions, Intelligence, Information and Service, Raytheon
1:00 – 1:15pm	**Transition to Breakouts**
1:15 – 2:00pm	**Breakout: Supply Chain Management** *Room 203* *States are thinking hard about how to secure an ever-growing list of vendors and third-party suppliers. This panel will discuss state initiatives to tackle this complex challenge and discuss how the private sector is also approaching supply chain as an example for states.*

Speakers:

- **Maggie Brunner**, Program Director, Homeland Security & Public Safety, National Governors Association (Moderator)

- **Nicholas Andersen**, State Chief Information Security Officer, Vermont

- **Chris Boyer,** Assistant Vice President, Global Public Policy, AT&T

- **Jon Check**, Senior Director, Cyber Protection Solutions, Cybersecurity and Special Missions, Intelligence, Information and Service, Raytheon

Breakout: Using Cyber Volunteers for Incident Response

Room 204

States must be prepared to deploy a trained and vetted cadre of cybersecurity professionals in the event of a cyber incident and often must be creative in ensuring surge capacity. Learn from two states who have introduced models for leveraging volunteers in the public sector and private sector to enhance responses to statewide cyber incidents.

Speakers:

- **Mary Catherine Ott**, Legislative Director, Homeland Security & Public Safety Committee, National Governors Association (Moderator)

- **David Cagigal**, State Chief Information Officer, Wisconsin

- **Chris DeRusha**, State Chief Information Security Officer, Michigan

- **Bill Nash**, State Chief Information Security Officer, Wisconsin

Breakout: How Does IT Centralization and Unification Improve Security?

Room 205

Many states have consolidated IT governance, but how has it affected security outcomes? This discussion will explore case examples from states to detail the cybersecurity benefits of a centralized and unified IT structure.

Speakers

- **Michael Garcia**, Senior Policy Analyst, Homeland Security & Public Safety, National Governors Association (Moderator)

- **Danielle Cox**, Acting State Chief Information Security Officer, West Virginia

- **Will Payne**, Senior Director for State, Local and Education Networking and Security, VMware

- **Deborah Snyder**, State Chief Information Security Officer, New York

- **Shane Swanson**, IT Security, North Dakota

2:00 – 2:15pm	**Break**
2:15 – 3:00pm	**Breakout: Coordinated Vulnerability Disclosures**

Room 203

Coordinated vulnerability disclosures are growing in popularity within the private sector and federal government but still have not seen wide adoption in states. This breakout brings together a research perspective on CVD programs and a state that is in the early stages of their own initiative.

Speakers:

- **Dan Lohrmann**, former State Chief Information Security Officer, Michigan (Moderator)

	- **James Collins**, State Chief Information Officer, Delaware - **Katie Moussouris,** Founder and Chief Executive Officer, Luta Security
	Breakout: Statewide Disruption Response Planning *Room 204* *Preparing for a high consequence cyber disruption demands coordination across many agencies and stakeholders. Learn how states institutionalized this coordination through their cyber disruption response plans.* *Speakers:* - **Michael Garcia**, Senior Policy Analyst, Homeland Security & Public Safety, National Governors Association (Moderator) - **Diego Curt**, Chief Compliance Officer, Idaho - **Major General Bret Daugherty**, Adjutant General, Washington National Guard - **Daniel Dister**, State Chief Information Security Officer, New Hampshire - **Maria Thompson**, State Chief Risk Officer, North Carolina
	Breakout: Information Sharing – How Far Have We Come? *Room 205* *Information sharing is an undying buzzword in cybersecurity that means different things to different people. Hear how you can enhance your information sharing capabilities and lessons learned from other states.* *Speakers:* - **Thomas MacLellan,** Director of Policy and Government Affairs, Symantec (Moderator) - **Deborah Blyth**, State Chief Information Security Officer, Colorado - **Aaron Call**, State Chief Information Security Officer, Minnesota - **Tom Duffy**, Director, Multi-State Information Sharing and Analysis Center
3:00 – 3:15pm	**Break**
3:15 – 4:15pm *Ballroom A/B*	**Lightning Talks** **What you Actually Need to Know about the Internet of Things** *Much has been said about the security implications of IoT, but what does that mean for state policymakers? This session will cover the business decisions states need to contemplate to anticipate the security risks IoT devices poses to their environments.* **Speaker:** - **Deral Heiland**, IoT Research Lead, Rapid 7 **After-Action on the Colorado Department of Transportation Ransomware Attack** *Colorado's Department of Transportation was hit with a massive ransomware attack in 2018, resulting in the first gubernatorially declared state of emergency due to a cyber incident, activation of the Emergency Management Assistance Compact (EMAC), and mobilization of the National Guard. Learn what happened during this event and how your state can apply lessons learned.* **Speaker:** - **Kevin Klein**, Director, Division of Homeland Security & Emergency Management, Department of Public Safety, Colorado

4:00 – 5:00pm *Ballroom A/B*	**State Efforts to Assist Locals with Cybersecurity** *State officials will detail how they are assisting local jurisdictions in enhancing their cybersecurity postures through longstanding programs like the Homeland Security Grant Program. This session will also provide insight on the role of the state government in supporting local cybersecurity.* ***Speakers:*** - **Brian Nussbaum**, Assistant Professor, University of Albany's College of Emergency Preparedness, Homeland Security and Cybersecurity (Moderator) - **Jeff Franklin**, Acting Director, Office of the Chief Information Officer, Iowa - **Brian Langley**, Executive Director, Department of Homeland Security, Indiana - **Shawn Talmadge**, Assistant Secretary, Public Safety and Homeland Security, Virginia - **Ben Voce-Gardner**, Director, Cyber Security, Division of Homeland Security & Emergency Services, New York
6:00 – 9:00pm *601 Spring Street (transportation provided)*	***American Electric Power* Reception**

Wednesday, May 15, 2019

7:30 – 8:15am *Ballroom C/D*	**Networking Breakfast**
8:15 – 8:45am *Ballroom A/B*	**Keynote and Awards Presentation for Cyber Youth Competition** *Speaker:* **Governor John Bel Edwards**, Louisiana
8:45 – 9:30am *Ballroom A/B*	**Panel: Preparing the Next Generation of Cybersecurity Professionals in Louisiana** *With a major deficit of cybersecurity professionals, state government and private sector partners need to work creatively and collaboratively to cultivate talent. This session will discuss how Louisiana is overcoming challenges associated with cybersecurity workforce development and how they are closing the gap for the skills of tomorrow.* ***Speakers:*** - **Governor John Bel Edwards,** Louisiana (Moderator) - **Dr. Rick Bateman**, Chancellor, Bossier Parish Community College - **Rick Gallot**, President, Grambling State University - **Dr. Les Guice**, President, Louisiana Tech University - **Yogesh Khanna**, Chief Technology Officer, General Dynamics Information Technology - **Ralph Russo**, Director, Information Technology Programs, Tulane University - **Craig Spohn**, Executive Director, Cyber Innovation Center

9:30 – 10:00am *Ballroom A/B*	**An Interview with Dan Geer** *Dan Geer is a world-renowned expert on information security and risk management. A trained statistician and electrical engineer, his numerous contributions to the field include the Kerberos protocol and MIT's Project Athena. He is the author of several books including the "Economics and Strategies of Data Security." This interview will cover a range of topics, including defining security and assess risks to the role of states.* ***Speakers:*** - **David Forscey**, Managing Director, Cybersecurity and Technology Program, The Aspen Institute - **Dan Geer**, Chief Information Security Officer, In-Q-Tel
10:00 – 10:15am	**Transition to Breakouts**
10:15 – 11:00am	**Breakout: Digital Identity – The Engine Empowering Digital Transformation** *Room 203* *Digital transformation is essential for government to enable improved service delivery, constituent engagement, and drive economic development. Constituents want a low-friction, high-value experience, from driver's license renewals to submitting validation for benefits. This session will discuss promising practices to foster digital identity management and strategies.* ***Speakers:*** - **Kevin Heckel**, Cyber Managing Director, Deloitte (Moderator) - **Erik Avakian**, State Chief Information Security Officer, Pennsylvania - **Derek Bridges**, Ohio Administrative Knowledge System Program Administrator, Ohio
	Breakout: Securing Homeland Security and Emergency Management Systems from Cyber Attacks *Room 204* *Homeland security and emergency management increasingly rely on IP-based technology when responding to natural and man-made disasters. Recently, these systems, such as emergency communications, have been targeted by malicious cyber actors to impede disaster and emergency response. This panel will discuss how states should account for protecting these systems.* ***Speakers:*** - **Michael Garcia**, Senior Policy Analyst, Homeland Security & Public Safety, National Governors Association (Moderator) - **Troy Mattern,** Vice President for Product and Services Cybersecurity, Motorola Solutions - **Ted Verren**, Director, Security Strategy and Planning, AT&T
	Breakout: Partnering to Protecting Critical Infrastructure *Room 205* *This session will discuss how state, federal, and private sector partners are addressing emerging cyber threats to critical infrastructure and future actions needed to bolster prevention, response, and recovery efforts.* ***Speakers:***

	- **Dan Lauf**, Program Director, Energy, Environment, and Transportation, National Governors Association (Moderator) - **Peter Bloniarz**, Executive Director, Cyber Security Advisory Board, New York - **Steve Swick**, Chief Information Security Officer, American Electric Power - **Bradford Willke**, Acting Director of Stakeholder Engagement and Cyber Infrastructure Resilience, U.S. Department of Homeland Security
11:00 – 11:15am	**Break & Transition**
11:15 – 12:00pm	**Breakout: Fighting Against the Greatest Vulnerability: Human Error** *Room 203* *Many successful cyber attacks are result of poor cyber hygiene by the operator of a system. Whether through phishing or weak passwords, cyber attackers exploit human users and operators to infiltrate and compromise IT systems. Learn why this is the case and how states can train their employees to better implement cyber hygiene and account for human-centric cybersecurity.* *Speakers:* - **Michael Garcia**, Senior Policy Analyst, Homeland Security & Public Safety, National Governors Association (Moderator) - **Dr. Margaret Cunningham**, Principal Research Scientist for Human Behavior, Forcepoint - **Jim Edman**, State Chief Information Security Officer, South Dakota - **Bhagwat Swaroop**, Executive Vice President of Industry Solutions and Business Development**,** Proofpoint
	Breakout: Confronting Cyber Crime *Room 204* *Learn how other states have established and sustained robust computer crime investigative units and explore recommendations to scale cyber crime enforcement.* *Speakers:* - **Maggie Brunner**, Program Director, Homeland Security & Public Safety, National Governors Association (Moderator) - **Jim Ellis,** Michigan State Police - **Jim Emerson**, Executive Director for Cyber Policy, National White Collar Crime Center - **Kristin Judge**, Chief Executive Officer and President, Cybercrime Support Network - **Drew Watts**, Assistant Special Agent in Charge, FBI New Orleans Field Office
	Breakout: Workforce Development *Room 205* *The cybersecurity industry faces an enormous workforce gap and is itself subject to potential disruption by new technology. This challenge provides a unique opportunity for innovative approaches at the state level to promote cybersecurity in K-12 education, prepare postsecondary students for cybersecurity careers, and implement public-private partnerships to develop the workforce development pipeline.* *Speakers:* - **Doug Robinson**, Executive Director, National Association of State Chief Information Officers (Moderator) - **Major General Courtney Carr**, Adjutant General, Indiana

	- **Jason Mangold**, Manager, Strategic Workforce Development, CompTIA - **Rodney Petersen**, Director, National Initiative for Cybersecurity Education
12:00 – 12:30pm *Ballroom C/D*	**Break into Lunch**
12:30 – 1:00pm *Ballroom A/B*	**Lunch Presentation: Ukraine Post-Mortem** *In December 2015, Ukraine suffered the first, publicly known cyber attack that created widespread blackouts throughout the country. Hear what happened and the implications for state efforts to secure critical infrastructure.* *Speaker:* - **Jonathan Homer,** Chief of the Industrial Controls System, Cybersecurity & Infrastructure Agency, U.S. Department of Homeland Security
1:00 – 1:30pm *Ballroom A/B*	**Keynote** - **Christopher Krebs**, Director, Cybersecurity & Infrastructure Security Agency, U.S. Department of Homeland Security
1:30 – 2:00pm *Ballroom A/B*	**Advanced Persistent Threats and How to Counter Them: A Conversation with John Carlin and Curtis Dukes** *John Carlin most recently served as Assistant Attorney General for National Security within the U.S. Department of Justice where he focused on a myriad of cyber criminal cases. He is joined by Curtis Dukes, the Executive Vice President and General Manager of the Best Practices and Automation Group at the Center for Internet Security. Prior to CIS, he served as the Deputy National Manager for National Security Systems within the NSA.* *Speakers:* - **John Carlin**, Chair, Cybersecurity & Technology Program, Aspen Institute - **Curtis Dukes**, Executive Vice President for Security Best Practices, Center for Internet Security
2:00 – 2:15pm	**Break**
2:15 – 3:00pm *Ballroom A/B*	**The National Guard and Cybersecurity** *Since the founding of the United States, National Guard units have been used to assist in preparing for, responding to, and recovering from nearly every conceivable natural and man-made disaster. Now, they are being used for cybersecurity missions. Federal and state subject matter experts will discuss the challenges and opportunities inherent to leveraging the National Guard for cybersecurity activities.* **Speakers:** - **Mary Catherine Ott**, Legislative Director, Homeland Security & Public Safety Committee, National Governors Association (Moderator) - **Adam DiPetrillo**, Commander, Cyber Mission Assurance Teams, Washington - **Colonel George Haynes**, Chief, Cyberspace Operations, National Guard Bureau - **Brigadier General Maurice McKinney**, Director of Cyberspace Operations, Missouri - **Michael Pruett**, Cybersecurity Director, Alabama

3:00 – 3:30pm *Ballroom A/B*	**Cyber Command's Mission** - **Major General Stephen J. Hager**, Mobilization Assistant to the Commander, U.S. Cyber Command, Deputy Commander of Operations, Cyber National Mission Force
3:30 – 3:45pm	**Break**
3:45 – 4:30pm *Ballroom A/B*	**Election Security: Looking Back, Looking Forward** *Securing election infrastructure has become a national priority since 2016 and was a prime emphasis in states for the 2018 elections. This session will review the lessons learned from the 2018 elections and explore their application during the 2020 election season.* ***Speakers:*** - **Michael Garcia**, Senior Policy Analyst, Homeland Security & Public Safety, National Governors Association (Moderator) - **Kyle Ardoin**, Secretary of State, Louisiana - **Phil Bates**, Chief Information Security Officer, Utah - **Robert Giles**, State Election Director, New Jersey - **Matt Masterson**, Senior Advisor on Election Security, U.S. Department of Homeland Security
4:30 – 5:15pm *Ballroom A/B*	**Fireside Chat** - **Jeff McLeod**, Director, Homeland Security & Public Safety, National Governors Association (Moderator) - **Governor Asa Hutchinson,** Arkansas - **Dr. Thomas Kennedy,** Chief Executive Officer, Raytheon
5:15pm	**Adjourn**
6:00 – 9:00pm *The Stage* *(transportation provided)*	**Louisiana Night (hosted by Cyber Innovation Center)**

Thursday, May 16, 2019	Optional Site Visit at the Cyber Innovation Center
8:00 – 8:30am	**Arrival and Check-in**
8:30 – 9:00am	**Breakfast, Welcome, and Introductions**
9:00 – 9:30am	**Cyber Innovation Center Overview** - Attendees will learn about the history of the National Cyber Research Park; the CIC's partnership with various stakeholders to foster economic development, R&D, and the facility's capabilities; and the National Integrated Cyber Education Research Center.
10:30 – 11:15am	**Visitors' Interest and Feedback**
11:15 – 11:30am	**Final Questions and Answers**
11:30am – 12:00pm	**Brief Tour**
12:00pm	**Adjourn**