National Summit on State Cybersecurity

June 22-24, 2022

Sheraton Columbus Hotel at Capitol Square | Columbus, Ohio

Meeting Materials

Scan the QR code to access resources and materials for this meeting, including the most up-to-date agenda.

National Summit on State Cybersecurity

Day 1 (Wednesday, June 22)

11:30 a.m. – 12:30 p.m.	**Registration and Lunch** *Congressional Room*
12:30 – 12:45 p.m.	**Color Guard, Welcome, and Overview** *Governor's Ballroom* ***Speaker*:** - *Bill McBride, Executive Director, National Governors Association*
12:45 – 1:00 p.m.	**Governor's Welcome** *Governor's Ballroom* ***Speaker:*** - *Governor Mike DeWine, Ohio*
1:00 – 1:30 p.m.	**Fireside Chat with Arkansas Governor Asa Hutchinson** *Governor's Ballroom* ***Speakers:*** - *Bill McBride, Executive Director, National Governors Association* - *Governor Asa Hutchinson, Arkansas*
1:30 – 2:30 p.m.	**Cybersecurity and the Whole-of-State Approach** *Governor's Ballroom*

Cybersecurity incidents have evolved well beyond the mere breach of personal data. Consequently, collaboration is key between state agencies, localities, public and private utilities, private companies, universities, hospitals, and more. In this session, North Carolina will serve as a case study for how states can employ a whole-of-state approach to confront cyber threats implicating such interests as homeland security, the local economy, and public health.

Speakers:
- *Doug Robinson, Executive Director, National Association of State Chief Information Officers, Moderator*
- *Jim Weaver, Secretary & Chief Information Officer, North Carolina*
- *Rob Main, State Chief Risk Officer, North Carolina*
- *Lieutenant Colonel Robbie Felicio, Chief Information Officer, North Carolina Army National Guard*
- *Lieutenant Colonel Seth Barun, Chief of Cyber Operations, North Carolina Army National Guard*

2:30 – 3:00 p.m. **Combatting Cyberattacks Through Public and Private Sector Collaboration**
Governor's Ballroom

State and local governments, which have faced a skyrocketing number of cyber and ransomware attacks, must juggle this constant threat with an expectation to handle growing amounts of constituent data and sensitive information. Gordon Bitko (formerly Chief Information Officer at the Federal Bureau of Investigation) and Dr. Michele Myauo will discuss ways industry can support state and local governments facing the threat of cyberattacks by sharing risk information, assisting with incident response procedures, and helping governments adopt cybersecurity best practices.

Speakers:
- *Gordon Bitko, Senior Vice President of Policy for Public Sector, ITI*
- *Michele Myauo, Ph.D., Managing Director, North America Public Services Security, Accenture*

3:00 – 3:30 p.m. **Networking Break**

3:30 – 4:30 p.m. **Civilian Cyber Corps: A Model for Collaboration, Preparedness, and Response**
Governor's Ballroom

Cybersecurity workforce shortages and resource constraints have led some states to turn to teams of volunteers to strengthen cyber incident response activities and mitigate losses. Some have even begun to offer proactive cyber assessment services to organizations across the state. This panel convenes three leaders to discuss the strengths and challenges of their states' programs and the diverse ways this model can be leveraged to address a growing number of cybersecurity needs across the community.

Speakers:
- *Steve Fugelsang, Cybersecurity Program Director, National Governors Association, Moderator*
- *Laura Clark, Chief Information Officer & Chief Security Officer, Department of Technology, Management & Budget, Michigan ([Michigan Cyber Civilian Corps (MiC3)](#))*
- *Alan Greenberg, Chief Information Security Officer, Wisconsin ([Wisconsin (Cyber Response Team (CRT) Program)](#))*
- *Major General John C. Harris, Jr., Adjutant General, Ohio National Guard ([Ohio Cyber Reserve](#))*

Scan here to access NGA's latest publication on this topic

4:30 – 5:00 p.m.	**Keynote: Artificial Intelligence & Cybersecurity** *Governor's Ballroom* *The promise of AI and the expansion of compute has paved the path for deployment across key business functions and industry verticals, enabling insights and automation of complex tasks at greater scale at speed. In this talk, Stephanie will provide a bridge from your current thinking on the promise of AI to the realities of the security risk and landscape, empowering thoughtful partners in understanding the risk we face in AI.* **Speaker:** - *Stephanie Domas, Chief Security Technology Strategist, Intel*
5:30 – 7:30 p.m.	**Evening Reception – Sponsored by American Electric Power** *Ohio Statehouse*

Day 2 (Thursday, June 23)

7:30 – 8:30 a.m.	**Networking Breakfast** *Congressional Room*
8:30 – 9:30 a.m.	**Secure from the Start: Prioritizing Cybersecurity in Energy and Critical Infrastructure Investments** *Governor's Ballroom* *Governors across the country are preparing to invest in and upgrade critical infrastructure systems across the country to meet a range of policy goals and leverage billions of dollars from the bipartisan Infrastructure Investment and Jobs Act. Experts in this panel will discuss how to optimize these investments and ensure that they are designed to be cybersecure at the outset, not as an afterthought.*

Speakers:
- *Charlie Lewis, Expert Associate Partner, McKinsey & Company, Moderator*
- *Mujib Lodhi, Chief Information Officer and Senior Vice President of Customer Experience, Long Island Power Authority*
- *Steve Swick, Vice President and Chief Security Officer, American Electric Power*
- *Andrew Kling, Vice President, Cybersecurity, Schneider Electric*

9:30 – 10:15 a.m.	**Insights from the Field: State Cyber Disruption Planning & Incident Response** *Governor's Ballroom* *Preparing for a high-consequence cyber disruption demands coordination across many agencies and stakeholders. Learn how states have institutionalized this coordination through strategic cyber disruption response planning.* **Speakers:** - *Timothy Blute, Director, Center for Best Practices, National Governors Association, Moderator* - *Major General Richard R. Neely, Adjutant General, Illinois National Guard* - *Jeff Brown, Chief Information Security Officer, Connecticut*
10:15 – 10:45 a.m.	**Networking Break & Transition**

10:45 – 11:30 a.m.

Transformation Through Digital Government and Identity Management *Governor's Ballroom*	**Strategies and Trends to Prevent and Survive a Ransomware Attack** *Judicial Room*	**Coordination for Electric Sector Cybersecurity** *Senate Room*
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:**	*Can your state agency afford and survive a ransomware attack? With all states and territories confronting a persistent ransomware threat, panelists will describe new and emerging trends in ransomware prevention, reflect on takeaways from response efforts, and discuss how states can bolster their cyber resilience now.* **Speakers:** - *Marty Edwards, Vice President of Operational Technology*	*A reliable supply of electricity is paramount for the safety, health, and economic viability of communities. As the sector faces increased cybersecurity threats, panelists in this session will explore opportunities for coordination between the states, electric sector, and federal government to ensure cyber preparedness and resilience.* **Speakers:** - *Dan Lauf, Energy Program Director, National Governors*

- *Kevin Heckel, Advisory Managing Director, Deloitte, Moderator*
- *Anupam Srivastava, State Chief Information Security Officer, Ohio*
- *Neal Gallucci, Technical Administrator, InnovateOhio Platform, Ohio*

Security, Tenable, Moderator
- *Erik Avakian, Chief Information Security Officer, Pennsylvania*
- *Steve Ocepek, Distinguished Engineer, Chief Technology Officer, Offensive Security, IBM*

Association, Moderator
- *Michael Geraghty, Chief Information Security Officer and Director, New Jersey Cybersecurity and Communications Integration Cell*
- *Sean Parcel, Director, Cyber Intelligence & Defense, American Electric Power*
- *Cynthia Hsu, IT Cybersecurity Specialist Office of Cybersecurity, Energy Security, and Emergency Response (CESER), U.S. DOE*

11:30 a.m. – 1:00 p.m.	**Lunch** *Congressional Room*

1:00 – 1:45 p.m.

Securing Homeland Security and Public Safety Emergency Management Systems
Senate Room

Homeland security and emergency management rely on IP-based technology when responding to natural and man-made disasters. 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

Software and IT Supply Chain Management to Overcome Near- and Long-Term Vulnerabilities
Judicial Room

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 how the private sector is approaching supply chain as an example for the states.

Speakers*:*

Cyber Workforce Development Workshop
Legislative Room

COVID-19, the Great Resignation, and the evolving security landscape have presented organizations with unprecedented workforce challenges. This workshop provides an opportunity to collaborate with your colleagues from other states to develop actionable solutions to address the widening cybersecurity workforce gap in government and

approach the protection of these systems.

***Speakers**:*
- *Steve Fugelsang, Cybersecurity Program Director, National Governors Association, Moderator*
- *Jay Kaine, Director, Cyber Threat Fusion Center, Motorola Solutions*
- *Brian Maholic, Director of the FirstNet Missions Critical Solutions, FirstNet Built with AT&T*

- *Henry Young, Directory, Policy, BSA | The Software Alliance, Moderator*
- *Adam Ford, Chief Information Security Officer, Illinois*
- *Paul Kurtz, Chief Cybersecurity Adviser, Splunk*

become a competitive employer of choice.

***Speakers**:*
- *Casey Dolen, Senior Policy Analyst, National Governors Association*
- *Meredith Ward, Director of Policy & Research, National Association of State Chief Information Officers*
- *Sarah Benczik, Principal, Deloitte*

1:45 – 2:00 p.m.	**Break**	

2:00 – 2:25 p.m.   **Keynote: Cybersecurity Trends, Strategies, and Success Factors for Securing Government**
Governor's Ballroom

Through storytelling, Palo Alto Networks' Cybersecurity Strategist Fadi Fadhil (former CIO of the City of Minneapolis, former CIO of Minneapolis Public Schools, and former Director of IT for St. Paul Public Schools) will share an overview of cybersecurity trends and themes, strategy highlights, and critical success factors for securing government post-2020.

Speaker:
- *Fadi Fadhil, Cybersecurity Strategist, Palo Alto Networks*

2:30 – 3:15 p.m.   **The National Guard: A Model for Partnership**
Governor's Ballroom

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 manmade disaster. Now, they are being used for cybersecurity missions. Federal and state subject matter experts will discuss the challenges and opportunities inherent in leveraging the National Guard for cybersecurity activities.

Speakers:
- *Michael Horder, Legislative Director, National Governors Association*
- *Colonel Thomas Pries, Washington National Guard*
- *Lieutenant Colonel Robert Lejeune, Wyoming National Guard*

3:15 – 3:45 p.m.   **Networking Break**

3:50 – 5:00 p.m.   **State-Local Partnerships in Cyber Resilience: Perspectives on Using State, Local, Tribal, and Territorial Grant Funds for Cyber Improvements**
Governors Ballroom

State-local partnerships to enhance whole-of-state cybersecurity resilience are a key priority area for state cybersecurity leaders. Panelists will discuss current efforts, priority areas, and takeaways from collaborative programming.

Speakers:
- *Carlos Kizzee, Senior Vice President, Stakeholder Engagement Operations, Center for Internet Security (CIS), Moderator*
- *Kirk Herath, Cybersecurity Strategic Advisor, Office of Governor Mike DeWine, Ohio*
- *Jeff Maxon, Chief Information Security Officer, Kansas*
- *Stephanie Helm, Director, MassCyberCenter, Massachusetts Technology Collaborative, Massachusetts*
- *Tracy Barnes, Chief Information Officer, Indiana*

5:15 – 7:00 p.m.   **NGA-Sponsored Happy Hour**
Buckeye Bourbon House

Day 3 (Friday, June 24)

7:30 – 8:30 a.m.   **Networking Breakfast**
Congressional Room

8:30 – 9:15 a.m.   **Risk Management, Cyber Insurance, and Controlling Costs**
Governor's Ballroom

An essential part of today's cybersecurity strategy is managing risk. Cyber insurance is one key component. Unfortunately, due to the dramatic increase in cybersecurity claims, the cyber insurance landscape has shifted making it more difficult to obtain, secure the right amount of coverage and more. This session will bring everyone with an interest in state and local government risk management mitigation up-to date on the latest developments, strategies, and workarounds.

Speakers:
- *Dr. Alan R. Shark, Vice President, Public Sector and Executive Director, CompTIA Public Technology Institute, Moderator*
- *Dan Lohrmann, Field Chief Information Security Officer, Presidio; former Chief Security Officer, Michigan; co-author of Cyber Mayday and The Day After*

- *Adam Frumkin, Certified Government Chief Information Officer (CGCIO), Chief Information Officer, Franklin County Data Center*
- *Erin Rian, Chief Operating Officer, National League of Cities Mutual & Risk Information Sharing Consortium (NLC Mutual-RISC)*

9:15 a.m. – 10:00 a.m.	**Cybersecurity Issues Affecting Hospitals and Healthcare Providers**

Governor's Ballroom

Healthcare organizations face constant cyber threats that put patient safety and human life at risk. Cyber resilience is critical to seamless healthcare delivery, the protection of healthcare systems, and medical device safety. There are also preparedness and response lessons to be gleaned from the 2020 cyberattack on Vermont's hospital system, in which National Guard assets featured prominently. Finally, a proliferation of ransomware poses risks to pharmaceutical supply chains and raises the prospect of shortages disrupting patient care.

Speakers:
- *Margie Zuk, Senior Principal Cybersecurity Engineer, MITRE, Moderator*
- *Suzanne Schwartz, M.D., Director, Office of Strategic Partnerships and Technology Innovation, Center for Devices and Radiological Health (CDRH), Food and Drug Administration*
- *John Riggi, National Advisor for Cybersecurity and Risk, American Hospital Association*
- *Brian Cincera, Chief Information Security Officer, Pfizer*

10:00 – 10:20 a.m.   **Keynote: Accelerated Need for "Zero Trust"**
Governor's Ballroom

The implicit trust inherent in any technology ecosystem needs to be systematically removed and replaced with an architecture that considers each user, device, and network as untrustworthy—until proven otherwise. Digital transformation, the shift to remote work, and the hybrid ecosystem have significantly accelerated the need for zero-trust architecture. In this session, Mr. Brahmapuram will unpack zero-trust architecture, discuss business use cases that drive adoption, and outline the steps needed to implement this architecture in your organization.

Speaker:
- *Vinod Brahmapuram, Senior Director, Security, Lumen Technologies; former Chief Information Security Officer, Washington*

10:20 – 10:35 a.m.   **Break**

10:35 – 11:35 a.m.   **Cloud Security and Supply Chain Risks**
Governor's Ballroom
The White House's Executive Order 14028 on Improving the Nation's Cybersecurity (issued May 12, 2021) requires agencies to enhance cybersecurity and software integrity and accelerate adoption of secure cloud services (e.g., 'zero trust' architecture). This panel will address how the private sector is approaching meeting

the requirements of Section 3 ("Modernizing Federal Government Cybersecurity") and Section 4 ("Enhancing Software Supply Chain Security"), and what state CIOs can do to meet current challenges.

Speakers:
- *Kris Winkler, Associate Director, Cybersecurity at Boston Consulting Group, Moderator*
- *Karen Worstell, Senior Cybersecurity Strategist, VMware*
- *Maria Thompson, State and Local Government Cyber Lead, Amazon Web Services*
- *Richard Pina, Head of State and Local Security Engineering, Google Cloud*

11:35 a.m. – 12:00 p.m.   **Grab-and-Go Lunch**

How did we do?

Please use the QR code to access a brief survey about your experience at this convening. Your feedback will help NGA improve future membership opportunities.

Share your thoughts by using #StateCyber on social media!