NGA Cybersecurity Newsletter

November 19, 2019

Contact: John Guerriero (jguerriero@nga.org)
202-624-5372

Resource Center Announcements

November Resource Center Webinar

Cyber Insurance: November 25th at 3:00pm ET

Please join us on **Monday, November 25th from 3:00 pm – 4:00 pm ET** for the next Resource Center webinar on Cyber Insurance. Every state and local government faces cyber risk, no matter their size. While cyber insurance can't protect your organization from a cybercrime, it can keep your organization on stable financial footing should a significant cybersecurity incident occur. Alan Shark, the Executive Director of the Public Technology Institute (PTI), will address what state and local governments should look for in a cyber insurance policy, what is typically covered in a cyber insurance policy and share best practices for state and local governments.

PTI works with a network of leading local officials to identify research opportunities, provide thought leadership and share solutions to the many technology issues that impact local government.

Please feel free to share this with any state and local partner. Contact Khristal Thomas (kthomas@nga.org) if you have any questions. Registration link is here and the Zoom link is here.

October Webinar on Ransomware and the Role of the MS-ISAC
During our October webinar, Brian Calkin, CTO for the Center for Internet Security, covered best practices for recovery, cyber hygiene tasks organizations can invest in and how stakeholders can leverage MS-ISAC to counter the risks associated with ransomware attacks. Slides (PDF) and a recording (MP4) are available.

NGA Information Requests:

1. How is your state using DHS's Homeland Security Grant Program (HSGP) funds for cybersecurity? Do you currently have a statewide program for the benefit of local entities? If you have already launched projects, what promising practices and lessons learned can you share? Please reach out to Maggie Brunner here.

2. What is your state National Guard's parameters for supporting election cybersecurity? If you would like to share more about your Guard's current efforts, please feel free to reach out to Maggie Brunner here.

3. How is your state funding cyber forensic capabilities? If you have a creative approach or promising practice, please reach out to Maggie Brunner here.

4. How is your state incentivizing or supporting government agencies and businesses in your jurisdiction to adopt the NICE framework? Please reach out to John Guerriero with promising practices here.

Cybersecurity Resources

CISA Releases Framework of Cyber Essentials

Consistent with the NIST Cybersecurity Framework, CISA's Cyber Essentials are a guide for leaders of small businesses as well as small and local government agencies to develop an actionable understanding of where to start implementing organizational cybersecurity practices. The framework can help organizations start envisioning a culture of cyber readiness, as well a set of actions steps for building it.

States Release Toolkits for Local Governments

Colorado Governor's Office of Information Technology recently released a guidebook for local governments offering security recommendations and resources to help build resilience to cyber incidents.

The Louisiana Department of Education released a set of checklists for local officials to help prevent and secure against cyber incidents. Included are:

- Preventative Measures Checklist
- Indicators of Compromise Checklist
- Critical IT Task List for School Systems

Indiana Governor Eric J. Holcomb's Executive Council on Cybersecurity, under the leadership of the Indiana Department of Homeland Security, has developed the Indiana Emergency Manager Cybersecurity Toolkit for local government emergency managers to use as they navigate through the complexities of cybersecurity at a local level.

NGA Joins the National Association of Secretaries of State (NASS) in Supporting #TrustedInfo2020

NASS has launched a bipartisan education effort aimed at promoting state and local election officials as the trusted sources of election information. #TrustedInfo2020 aims to reduce the misinformation and disinformation surrounding elections by directing voters directly to election officials' websites and social media pages. NGA joins a host of other organizations in supporting NASS in this effort.

Cyber Workforce Development Resources

The Aspen Cybersecurity Group has convened a coalition of fifteen major companies who have agreed to adopt and implement principles to build a more robust pipeline for cybersecurity talent, including abandoning requirements for four year college degrees and implementing the NICE framework. The coalition will focus on ways to continue developing talent pipelines, re-assessing job specifications, and making career pathways more understandable. Read more about the Aspen Cybersecurity Group here.

Accenture recently released the results of an apprenticeship survey targeting community college students across the U.S. The findings demonstrate that a majority of students desire to pursue in-demand tech professions, including cybersecurity, and consider apprenticeship programs to be one of the best pathways to access those positions. The survey was designed to better understand students' career aspirations and to identify how employers can leverage apprenticeship programs to tap into this diverse talent pool.

Cybersecurity News

Ohio Governor Creates Civilian Cyber Reserve

Ohio Governor Mike DeWine signed a bill creating the Ohio Cyber Reserve – a civilian cyberforce within the Ohio National Guard capable of responding to cyberattacks against election systems, governments, businesses, and critical infrastructure. The state is now taking applications from civilians with internet and high-tech security skills to join the special unit. Read more here.

Federal Agencies Release Joint Statement on Election Security

The DOJ, DOD, DHS, DNI, FBI, NSA, and CISA released a joint statement on ensuring the security of the 2020 elections. Read the full statement here.

USDA and Department of Energy Join Forces to Increase Energy Technology Development and Deployment in Rural America

U.S. Department of Agriculture (USDA) and U.S. Department of Energy (DOE) announced a MOU to promote rural energy and the development of technologies that will support and advance rural and agricultural communities. USDA and DOE have convened interagency working groups to focus on five major areas, including supporting and investing in cyber security initiatives and grid improvement.

Federal Cyber Exercises Test Critical Infrastructure

On November 13-14, several states participated in GridEx V – the North American Electric Reliability Corporation (NERC) exercise designed for utilities to demonstrate how they would respond to and recover from simulated cyber and physical security threats and strengthen their crisis communications processes. Over 425 organizations participated in the exercise. Read more here.

The Securities Industry and Financial Markets Association (SIFMA) recently completed an exercise as part of “Quantum Dawn”, a series designed to simulate a catastrophic cyber event in the banking sector. The exercise included around 800 participants from major financial institutions and regulators, including participants from Europe and Asia – a first for a Quantum Dawn exercise. The scenario outlined what would occur if ransomware attack targeted the global financial system. Read more here.

FBI Holds Ransomware Summit

The FBI convened top ransomware experts for a closed-door summit in September to better facilitate private sector data sharing to combat the growing ransomware threat. Hosted by Carnegie Mellon University and facilitated by the National Cyber-Forensics and Training Alliance, the discussion topics included which type of information would be most valuable for the private sector to share with the FBI, as well as briefings on ransomware investigations and the prosecution process. Read more here.

FCC Inquiry on Huawei Gear Near U.S. Military Bases

The Federal Communications Commission (FCC) is planning to assess locations where Huawei equipment has been installed, with special attention to those in close proximity to U.S. military bases. Read more here.

Updates from NGA Advocacy

The Senate Homeland Security Committee recently approved a bill that would help local governments move .gov domain, which is validated by the federal government. The legislation (S. 2749) will allow local governments to use the Homeland Security Grant Program to reimburse the expense of switching domains. The legislation is sponsored by Chairman Ron Johnson (R-WI), Gary Peters (D-MI), Amy Klobuchar (D-MN), and James Lankford (R-OK).

The Senate also passed a bill (S.1388) mandating that government officials with supply chain responsibilities receive counterintelligence training. The bill is also sponsored by Chairman Ron Johnson (R-WI) and Gary Peters (D-MI).

NGA Resource Center for State Cybersecurity Partners

- American Electric Power
- Anomali
- AT&T
- CompTIA
- Deloitte
- Google Cloud
- Proofpoint
- Rapid7
- Raytheon
- Splunk
- Symantec
- Tenable
- VMware