NGA Cybersecurity Newsletter

July 1, 2021
Contact: John Guerriero (jguerriero@nga.org)
202-624-5372

Resource Center Announcements

ResCon Registration Now Live

ResCon, the premier annual international conference on the practice of successful resilience and disaster management, is scheduled for **September 15 – 17**, **2021** in New Orleans, Louisiana. The conference's three days of programming will focus on COVID-19 response and recovery, climate change resilience, serving vulnerable populations and cybersecurity and infrastructure. A preliminary agenda can be found here.

In partnership with NGA, ResCon is offering complimentary registration to Governors and one member of their administration, such as a homeland security advisor, chief resilience officer or energy policy advisor. Upon approval of your Governor's office, you may register using a discount code reserved for gubernatorial staff. Please reach out to John Guerriero here with any questions regarding that. The general registration link here.

NGA Launches Governors' Cybersecurity Communications Campaign

NGA recently launched a campaign to feature Governors' messages on the vital role of cybersecurity in protecting critical assets and the information security of the public. Please send any communications activities on cybersecurity you would like to have featured by NGA to John Guerriero here.

Webinar: Addressing Energy Security Through State Cyber Governance Bodies

As the energy cybersecurity threat landscape continues to evolve and our dependency on digital and connected technology grows, Governors are increasingly focusing on addressing cybersecurity vulnerabilities in their states, including the energy sector. NGA recently summarized eight states' activities in forming cybersecurity governance bodies addressing the energy sector in a white paper and recently held a webinar featuring Indiana and Louisiana. Slides and a recording can be found here.

Requests for Information:

GAO Request for Information on Federal Assistance for State and Local Governments with Ransomware

The U.S. Government Accountability Office (GAO) is conducting research in response to a congressional request on the federal government's efforts to provide ransomware assistance to state and local governments and the extent to which those efforts include coordination across the federal government. As part of this work, GAO is seeking information from state or local government organizations that obtained ransomware-related assistance from one or more federal agencies. The full GAO request can be found here and if you are interested in discussing your experiences with the GAO, please let John Guerriero know by **July 15, 2021**.

Ohio Cybersecurity Qualitative Survey

The Ohio Homeland Security Division is conducting a qualitative survey on state cyber centers. They are seeking responses to five questions on state cybersecurity. For more information, including the list of questions and who to respond to, please see the document here.

Cybersecurity Resources

NACo Cybersecurity Priorities and Best Practices

The National Association of Counties (NACo) released its Cyber Security Priorities and Best Practices guide. Each priority is broken down by percentage of cost, cyber defense impact, and workload effort to implement the priority areas. Read more here.

CISA Vulnerability Disclosure Policy (VDP) Platform

CISA announced its Vulnerability Disclosure Policy (VDP) Platform that will support federal agencies with the option to use a centrally-managed system to collaborate and receive information on vulnerabilities from the public to improve the security of their internet-accessible systems. Read more here.

CISA Releases Ransomware Readiness Assessment

CISA released a Ransomware Readiness Assessment (RRA) module, a self-assessment based on a tiered set of practices that will help organizations assess their ability to defend against and recover from a ransomware incident. Tailored for different maturity levels, the RRA can be valuable to most organizations regardless of their cyber maturity. Read more here.

Report on Cyber Threat to Operational Tech from USB Devices

Honeywell recently released a report examining the cybersecurity threat posed by USB devices to operational technology (OT) environments. The report found that nearly 80% of cyber threats from removable devices could critically impact OT and that nearly 40% of all cybersecurity threats were designed to use removable devices – a large increase from previous years. Read more and access the full report here.

NICE Summer e-Newsletter Released, NGA Policy Academy Spotlighted

The National Initiative for Cybersecurity Education (NICE) released its Summer 2021 e-Newsletter and features the 2021 NGA Policy Academy. Read the newsletter here the Policy Academy spotlight here.

Cybersecurity News

Governor Hutchinson Forms Cyber Advisory Council

Arkansas Governor Asa Hutchinson signed an executive order creating the Arkansas Cyber Advisory Council to identify and manage the risk of cyberattacks and to enhance the state's response efforts. Among other duties, the cross-disciplinary council will look to develop a roadmap for improving the state's cybersecurity culture, improve collaboration between state agencies and strengthen threat protection and detection capabilities. The council will provide recommendations to the Governor and the state legislature. Read the order here and the Governor's press release here.

White House Official Briefs State AGs on Private-Sector Role Battling Ransomware

In a meeting with the National Association of Attorneys General, Deputy National Security Advisor for Cyber and Emerging Tech Anne Neuberger discussed how the Biden administration is leveraging state attorneys offices to help counter the ransomware wave and stressed private-sector collaboration as crucial to the success of its strategy to reduce ransomware's impact. Read more here.

DOJ Seizes Cryptocurrency Payments From Colonial Pipeline Ransomware Attack

The Justice Department announced that it has retrieved $2.3 million, a little over half of the original ransom payment that Colonial Pipeline made in the Colonial Pipeline ransomware attack. The agency seized 63.7 Bitcoin from the 75 paid by Colonial. Read the DOJ release here.

FBI Asks Congress For $40M To Help Combat Wave Of Ransomware

During a Senate Panel on June 23, FBI Director Christopher Wray told lawmakers that a request for a $40 million increase in its cybersecurity budget for the upcoming fiscal year would go in part towards combating increasing and damaging ransomware attacks. Read more here.

JBS Attack Renews Discussion on Cybersecurity in Food Supply Industry

The recent ransomware attack against global meatpacking company JBS renewed the discussion assessing the vulnerability of the U.S. food supply industry. This Politico report examines the lack of mandatory cybersecurity rules governing the industry and the need for enhanced protections and protocols to be put in place. Read more here.

Cyber Yankee Exercise Convenes New England Soldiers and Airmen

Marine and National Guard cyber operators from around New England gathered at Joint Base Cape Cod to participate in the seventh annual Cyber Yankee cybersecurity exercise with the goal to enhance their ability to defend against malicious actors in the digital space. Read more about the exercise here.

Texas Launches Volunteer Cyber Incident Response Team

Texas Governor Abbott recently signed legislation creating a volunteer incident response team. A few states have similar programs, including the Michigan Cyber Civilian Corps (MiC3) formed in 2014, to support state efforts to supplement the state response with civilian assistance. Read more here.

NGA Government Relations Updates

Senate Confirms National Cyber Director

The Senate confirmed Chris Inglis on June 17 as President Biden's Cyber Director, heading up the new Office of the National Cyber Director within the White House. Director Inglis will look to coordinate the cybersecurity work done across various federal agencies and lead the development of the national digital defense strategy. Read more here.

President Biden Outlines Steps to Strengthen Critical Supply Chains

President Biden released a multi-pronged strategy to secure critical supply chains. The administration will establish a supply-chain disruptions task force to address near-term bottlenecks that can affect economic recovery. Commerce Secretary Gina Raimondo, Transportation Secretary Pete Buttigieg, and Agriculture Secretary Tom Vilsack head the team focusing on supply-demand mismatches in several markets, including semiconductors, transportation and agriculture. The White House released a 250-page report with assessments and an expansive list of recommendations.

Read the White House's press release here and the larger Supply Chain Report here.

K-12 Cybersecurity Legislation Introduced

Representative Doris Matsui (D-CA), along with Representatives Jim Langevin (D-RI), John Katko (R-NY) and Andrew Garbarino (R-NY), introduced the Enhancing K-12 Cybersecurity Act. The legislation would look to create a cyber information exchange, a registry of cyber incidents impacting K-12 schools and a K-12 cybersecurity technology improvement program. Read more about the bill here and the view the full text here.

Lawmakers Look to Create Cyber Training Programs At CISA, VA

Senators Maggie Hassan (D-NH) and John Cornyn (R-TX) are co-sponsoring the Federal Cybersecurity Workforce Expansion Act, which create a registered apprenticeship program at CISA and a veteran training pilot at the Veterans Administration. Read more about the bill here and view the full text here.