NGA Cybersecurity Newsletter

July 30, 2021
Contact: John Guerriero (jguerriero@nga.org)
202-624-5372

Resource Center Announcements

Arkansas Governor Asa Hutchinson Becomes Chairman of NGA, New Jersey Governor Phil Murphy Elected Vice Chairman

Arkansas Governor Asa Hutchinson was elected as NGA chairman and after a vote of his fellow governors, New Jersey Governor Phil Murphy became the NGA vice chairman, with a role overseeing the NGA Center for Best Practices. The Governors assumed their new roles during the NGA Summer Meeting, which took place in a virtual format. Read more in NGA's press release here.

Governors Discuss Cybersecurity with DHS Secretary Mayorkas

At the NGA Summer Meeting, NGA Pandemic and Disaster Response Task Force co-chairs Connecticut Governor Ned Lamont and Tennessee Governor Bill Lee led a discussion between governors and DHS Secretary Alejandro Mayorkas on recent high-profile cyber attacks and the urgency to prioritize federal and state coordination on prevention and response. View the discussion on NGA's YouTube page here.

President Biden Appoints Council of Governors

President Biden appointed 9 governors to the Council of Governors, who will join incumbent Tennessee Governor Bill Lee. The Council of Governors is a bipartisan body of 10 governors that will work with the Biden administration on issues that affect national security, homeland defense, cybersecurity, disaster response and recovery, and the National Guard. Read more in NGA's Release and the White House Release.

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 is here.

NGA Requests for Information:

1. If your state has established a formal cybersecurity taskforce or commission, what recommendations would you have for states looking to form their own? How were the body's recommendations presented and implemented?

Please reach out to John Guerriero here on the above requests or with any specific technical assistance requests.

Cybersecurity Resources

CISA Releases FY20 Risk & Vulnerability Assessment Analysis and VDP Platform

The Cybersecurity & Infrastructure Security Agency (CISA) released an infographic and analysis of the Risk and Vulnerability Assessment (RVA) findings from fiscal year 2020. Conducted across multiple sectors, the RVA documents potential attack paths that a threat actor could follow and details the successful techniques organizations can take to combat each tactic. See the infographic and analysis here.

CISA also announced it has launched a Vulnerability Disclosure Policy (VDP) platform to increase coordination between the federal civilian executive branch and the civilian security research community. The platform offers a single website that serves as the primary point of entry for intaking, triaging and routing any vulnerabilities that researchers disclose. Read more here.

Joint Advisories Issued on Top CVEs and Chinese State-sponsored TTPs

The FBI and CISA, along with the UK's National Cyber Security Centre and the Australian Cyber Security Centre, released a joint cybersecurity advisory detailing the top 30 Common Vulnerabilities and Exposures (CVEs) routinely exploited by malicious actors in 2020. The advisory includes technical details and mitigations as well as what CVEs organizations should prioritize in 2021.

CISA, the FBI and the NSA also released a joint advisory describing over 50 tactics, techniques, and procedures used by Chinese state-sponsored cyber actors. The advisory also offers mitigations. Read the advisory here.

CRS Insight: Department of Justice Efforts to Counter Ransomware

The Congressional Research Service (CRS) released a memo highlighting the Department of Justice's (DOJ) efforts to counter ransomware attacks and their potential damage. The DOJ has taken several steps to investigate, prevent, and raise awareness of these attacks. The DOJ created a Ransomware and Digital Extortion Task Force whose goals include developing better information-sharing among parties and stronger investigation into nation-state connections. Read the CRS memo here.

Department of Energy Releases Updated Cybersecurity Capability Maturity Model

The Department of Energy released Version 2.0 of the Cybersecurity Capability Maturity Model (C2M2) that includes information about developing threats like ransomware and supply chain disruptions. The model helps businesses and organizations assess and improve their cybersecurity capabilities. The original C2M2 model was released in 2012, and the update is built on input from over 70 energy companies and more than 140 cyber experts. Read more here.

Cybersecurity News

Governor Hogan Convenes Annapolis Cybersecurity Summit

Maryland Governor Larry Hogan convened a discussion with several senior government officials and industry leaders to discuss the key threats facing federal, state and local governments and the private sector. Speakers included NGA Resource Center for State Cybersecurity co-chairs Arkansas Governor Asa Hutchinson and Louisiana Governor John Bel Edwards, Deputy National Security Advisor Anne Neuberger and Congressman John Katko.

At the end of the event, Governor Hogan enacted several cyber initiatives, including a partnership with the NSA to have a senior level analyst advise the state; a memorandum of understanding with the University of Maryland, Baltimore County that establishes a Maryland Institute for Innovative Computing and creates joint cyber rapid response teams; and signed executive orders creating a Chief Data Officer, a Chief Privacy Officer and establishing a statewide privacy framework. Read more and watch a recording of the event here.

Governor Kelly Establishes the Governor's Cybersecurity Task Force

Kansas Governor Laura Kelly issued an executive order creating the Governor's Cybersecurity Task Force, comprised of 15 state, local, and agency leaders. The bipartisan task force will look to develop a comprehensive plan to protect the state's data and services. Read more about the Task Force, its membership and specific duties here.

Governor Lamont Signs Legislation Strengthening Cybersecurity in the Private Sector, Announces Historic Public Sector Investment

Connecticut Governor Ned Lamont signed into law Public Act 21-119, *An Act Incentivizing the Adoption of Cybersecurity Standards for Businesses*, which mandates that businesses that have adopted and adhered to appropriate cybersecurity measures are protected from punitive damages if personal or restricted information is improperly maintained, accessed, communicated, or processed. Gov. Lamont also announced an $11 million investment in Connecticut's enhanced cybersecurity efforts. Read more here.

Federal Government Launches StopRansomware.gov

Several federal agencies, including the DHS and DOJ, announced a new website to protect American businesses and communities from ransomware attacks. StopRansomware.gov is a one-stop hub for ransomware resources for individuals, businesses, and other organizations.

Cyber Insurance Industry Efforts to Combat Ransomware Attacks

The cyber insurance industry has been active recently in efforts to counter the ransomware wave. In June, seven top insurance companies formed CyberAcuView, an organization that combines their data collection and analysis powers to enhance risk mitigation. In July, the American Property Casualty Insurance Association released its guiding principles on ransomware and cyber extortion to control the rising threat. Read more here.

Higher Ed Institutions Collaborate on Virtual Cyber Institute

Through a $1.5M Department of Defense grant, Washington State University is working to create the Northwest Virtual Institute for Cybersecurity Education and Research in collaboration with the University of Idaho, Central Washington University, Montana State University, and Columbia Basin College. The Institute will offer four-year degree and certificate programs in various cybersecurity topics and host students, ROTC and DoD-skilled civilian workers. Read more here.

Local Public Works Officials Testify on Cyber Threats to Physical Infrastructure

In a meeting for the Senate Committee on Environment and Public Works, local public officials discussed the necessary cyber protections and barriers for drinking water and wastewater systems. Given the decentralized nature of the nation's water, enacting standard cybersecurity measures is a complicated objective. Several measures were discussed, including increased cybersecurity training, boosting existing resources, and possibly enacting regulations. Read more here, and find the hearing recording and transcript here.

Florida Department of Economic Opportunity Breached

The Florida Department of Economic Opportunity warned of a potential breach of its unemployment data. Around 58,000 accounts were targeted in a breach that lasted between April and July 2021. In a letter to potential targets, the DEO recommended they monitor their credit accounts for fraudulent activity. Read more here.

DARPA Makes Vulnerability Disclosure Platform for Ethical Hackers Open Source

The Defense Advanced Research Agency's (DARPA) hardware vulnerability disclosure platform for white-hat hackers, Finding Exploits to Thwart Tampering, is now open source. The Agency hopes that ethical hackers will spot flaws with chip design and aid the creation of new processor protypes. Read more here.

DHS Announces Cybersecurity Hiring Initiative

In May, DHS Secretary Mayorkas set a goal to hire 200 new cybersecurity personnel across the Department by July 1. Secretary Mayorkas recently announced the Department's largest cybersecurity hiring initiative in its history with the onboarding of nearly 300 cybersecurity professionals. The hiring initiative, which exceeded its goal by almost 50 percent, is part of a 60-day Cybersecurity Workforce Sprint focused on building a more diverse cybersecurity workforce. Read more here

NGA Government Relations Updates

$1 Billion in Cyber Grants Outlined in Senate Infrastructure Deal

The $1.2 trillion infrastructure package being negotiated between the White House and a bipartisan group of Senators includes key cyber provisions for state and local governments. According to a summary obtained by CNN, the deal includes a $1 billion dedicated grant program for improving state, local, tribal and territorial (SLTT) government cybersecurity, $100 million towards a CISA cyber response and recovery fund, and $35 million for CISA to establish oversight over government critical infrastructure. Read more here.

NGA, the Governors Homeland Security Advisors Council, and other state-local associations, sent a letter to House and Senate leadership requesting inclusion of a dedicated cybersecurity grant program for SLTT governments in any upcoming infrastructure and appropriations packages.

The House also passed H.R. 3138, The State and Local Cybersecurity Improvement Act, which would look to authorize an annual $500 million grant program to provide SLTT governments dedicated funding to increase their cyber resiliency. Read the bill here.

House Passes Bill on Industrial Control Systems Cybersecurity

The House passed H.R. 1833, the DHS Industrial Control Systems Capabilities Enhancement Act, which would require CISA to maintain certain capabilities to identify and address threats to industrial control systems. Read the bill here.

President Biden Issues National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems

The memorandum establishes an Industrial Control Systems Cybersecurity Initiative described as “a voluntary, collaborative effort between the federal government and the critical infrastructure community to significantly improve the cybersecurity of these critical systems.” The memo also directs DHS to develop and issue cybersecurity performance goals for critical infrastructure. CISA and NIST will lead the effort. Read the memorandum here.

DHS Announces Allocations for FY21 Preparedness Grants

The Department of Homeland Security (DHS) and the Federal Emergency Management Agency (FEMA) announced the final allocations for $475 million for seven FY 2021 competitive preparedness grant programs. These allocations, together with the almost $1.5 billion in non-competitive grant funding announced earlier this year, total nearly $2 billion to help prepare against man-made threats and natural disasters. DHS identified four critical priority areas for attention: cybersecurity, soft targets and crowded places, domestic violent extremism, and emerging threats. Applicants under the grant programs were provided percentage increases in their competitive scores for aligning their projects around these areas. See the DHS advisory here and the FEMA advisory here.

Senate Confirms CISA Director

The Senate unanimously confirmed Jen Easterly as Director of DHS’ CISA. Director Easterly’s previous roles include serving as a special assistant to the president and senior director for counterterrorism at the National Security Council under President Obama. Read more about Director Easterly here and see her statement following being sworn in here.