NGA Cybersecurity Newsletter

October 29, 2021
Contact: John Guerriero (jguerriero@nga.org)
202-624-5372

Resource Center Announcements

NGA Webinar: Developing a Cybersecurity Curriculum for K-12 Schools

Please join NGA on **Tuesday, November 9th from 3:00 - 4:00pm ET** for a discussion with national and state experts on best practices for establishing cybersecurity concepts in K-12 schools. We'll be joined by Kevin Nolten, Director of Academic Outreach at CYBER.ORG, and officials from the State of Michigan.

Please register for the webinar here and reach out to John Guerriero with any questions here.

Previous NGA Webinar: Cybersecurity for the Water and Wastewater Systems Sector

On September 22nd, NGA hosted a webinar on Cybersecurity in the Water/Wastewater Critical Infrastructure Sector. The session was moderated by Tenable's Marty Edwards and featured Michael Arceneaux from the WaterISAC, Judith Germano of NYU's Center for Cybersecurity and Germano Law LLC, and Dr. David Travers from the U.S. Environmental Protection Agency. You can view a recording of the session here, the slides (which contain additional information on ARPA eligibility for the sector) here, and notes from the conversation here.

NGA Announces 4 States Participating in GridEx VI

NGA will support four states - **California, Connecticut, Illinois and Utah** – as they participate in the nationwide GridEx VI exercise, which reviews and tests energy emergency preparedness through a simulated coordinated cyber and physical incident on the electrical grid. NGA will work with cross-disciplinary teams from each of the four states in the lead up to, during, and after the exercise to develop and implement strategic action plans. Read NGA's release on the 2021 cohort here.

NGA Requests for Information:

- How has your state presented data on cybersecurity risk to agency leadership and/or elected officials? Are there recommendations for best visualizing that risk to non-technical audiences? Please reach out to John Guerriero here.

- Does your state have a policy prohibiting or accepting payments made in cryptocurrency? Please reach out to John Guerriero [here.](#)

- What is your state National Guard's capacity and process for supporting cyber incident response involving life-critical facilities like hospitals? If you are willing to share more about the Guard's capacity and Governor's policy/procedures for deploying cyber units, please reach out to Steve Fugelsang [here](#).

Cybersecurity Resources

NASCIO Releases 2021 State CIO Survey
> NASCIO has released its annual survey of state chief information officers, with this year's edition garnering feedback from officials from 49 state and territories. The survey explores several themes, including the impact of the COVID-19 on state services, digitizing services, broadband and wireless connectivity and legacy modernization. Read the full survey [here](#).
>
> NASCIO also recently released a publication on how the COVID-19 pandemic shaped AI adoption in state government and what it may mean in the future. Read the white paper [here](#).

Local Governments Surveyed on Cybersecurity
> CompTIA's Public Technology Institute (PTI) released a national survey of local government cybersecurity programs and cloud initiatives, centering around budgeting, policies and procedures, access management, cyber insurance and leadership support. Resource allocation, rising cyber insurance rates and leadership engagement were among some of the areas of concern. See the survey [here](#)v.

Microsoft Digital Defense Report Explores Rising Threats
> Microsoft released its Digital Defense Report exploring the state of cyber crime and an overview of the cyber threat landscape. The report also looks at hybrid workforce security, disinformation, and the security of supply chains, IoT and operational technology. Read the report [here](#).

Higher Ed Efforts on Cybersecurity Recruiting
> EdScoop examines several strategies that educational institutions have taken to promote cybersecurity careers to students at the K-12 level and beyond. Strategies include apprenticeship programs, improving access to cyber ranges and using virtual reality to build cybersecurity skills for K-12 students. Read more [here](#).

Biden Administration Outlines Public Counter-Ransomware Efforts

The Biden White House released a fact sheet on the administration's efforts on countering ransomware. The efforts are organized along the following four lines of effort:

- Disrupt ransomware infrastructure and actors
- Bolster resilience to withstand ransomware attacks
- Address the abuse of virtual currency to launder ransom payments
- Leverage international cooperation to disrupt the ransomware ecosystem and address safe harbors for ransomware criminals.

The fact sheet lists the different actions the administration has taken in the past year on each of the four categories. Read the sheet here.

Federal Advisories Released

CISA and the National Security Agency (NSA) published a cybersecurity guidance for 5G cloud infrastructures. The guidance is one in a 4-part series on protecting against 5G infrastructure security challenges that were identified in an earlier analysis paper. This guidance focuses on preventing and detecting lateral movement within cloud networks. Read the guidance here.

CISA, the FBI and the NSA released a joint Cybersecurity Advisory on the actors behind BlackMatter ransomware, who have targeted U.S. critical infrastructure entities. Read the advisory and recommended mitigations here.

CISA, the FBI, NSA and the Environmental Protection Agency (EPA) issued an advisory highlighting malicious cyber activity targeting the U.S. Water and Wastewater Systems Sector. Read the advisory, technical details and the recommended mitigations here.

See the full list of US-CERT advisories, including the NOBELIUM advisory, here.

Cybersecurity News

Maryland Partners with NSA on Cybersecurity

Maryland Governor Larry Hogan announced that the State of Maryland and the National Security Agency have created and filled a position for a senior-level data analyst to advise the state on enterprise data practice, policies, standards and security. The creation of the position was announced earlier this year at Governor Hogan's Annapolis Cybersecurity Summit. Read more here.

Arizona Launches Cyber Command Center

Arizona Governor Doug Ducey announced the creation of a new statewide Cyber Command Center earlier this month. The new center will be the central coordinating point for statewide cyber operations and information

sharing while also serving as the intersection for local, state and federal agencies' collaboration on cyber incident prevention and response. Read more about the Cyber Command Center [here](#).

ONCD Issues Statement of Strategic Intent

The Office of the National Cyber Director (ONCD) released statement of strategic intent, laying out the new office's vision and priorities. The statement lists four main outcomes that the ONCD will look to accomplish with the collaboration of national and federal partners:
- Promoting coherence across the federal government in cyber policy, action and doctrine;
- Improving public-private collaboration to address cyber challenges across sectors;
- Aligning resources to aspirations for federal agencies' cyber initiatives and assets; and
- Increasing resilience, both for the present and the future.

Read the statement [here](#).

Tennessee IT Agency Working Towards Improving DEI

At the October NASCIO conference, Tennessee CIO Stephanie Dedmon discussed how Tennessee's Strategic Technology Solutions (STS) agency formed an internal council focusing on improving and promoting diversity, equity and inclusion (DEI) within the agency. The internal council's charter focuses on five areas: recruitment, outreach, inclusion, communications and analytics. The agency's efforts coincide with increased priority placed on the need for DEI in the cybersecurity field among state IT officials. Read more [here](#).

States Embrace Whole-of-State Approach to Cybersecurity

This GovTech article examines how the whole-of-state approach to cybersecurity has continued to gain traction with state governments. Efforts across Colorado, New York, North Carolina and Virginia are highlighted. Read more [here](#).

Hospitals Targeted by Russian-Speaking Cyber Actors

Cybersecurity firm Mandiant released a report detailing how FIN-12, a Russian-speaking cybercriminal group, has increasingly been targeting North American hospitals and healthcare organizations with ransomware. The report covers FIN-12's activity and its tactics, techniques and procedures. Read more [here](#).

NGA Government Relations Updates

K-12 Cybersecurity Act Signed into Law

President Biden signed S.1917, the K-12 Cybersecurity Act of 2021, into law earlier this month. The bill, which was sponsored by Senator Gary

Peters (D-MI), directs CISA to conduct a comprehensive study of the cybersecurity risks facing the K-12 community and then produce a toolkit to help schools improve their hygiene. Read the bill's text [here](#) and more about the bill [here](#).