NGA Cybersecurity Newsletter

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

Resource Center Announcements

October is **Cybersecurity Awareness Month**, and this year's theme is "Do Your Part. #BeCyberSmart." Read more about the NCSAM theme, schedule of events, and resources from the Cybersecurity Infrastructure Security Agency (CISA) here. Additionally, **Cybersecurity Career Awareness Week** will occur from October 18-23. Read more about the week-long campaign here.

Please feel free to send any news and information on your state's upcoming events to John Guerriero here.

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 Requests for Information:

- Does your state have any best practices on presenting cybersecurity risk to state leadership? Are there recommendations for best visualizing that risk to non-technical audiences?

- How has your state approached minimum standards and controls with local government entities? What mechanisms or processes established those?

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

Cybersecurity Resources

CISA Annual National Cybersecurity Summit Set for October

CISA is hosting its annual summit virtually again this year over the course of four Wednesdays in October. Each of the sessions will have different themes:

- Oct. 6 - Assembly Required: The Pieces of the Vulnerability Management Ecosystem
- Oct. 13 - Collaborating for the Collective Defense
- Oct. 20 - Team Awesome: The Cyber Workforce
- Oct. 27 - The Cyber/Physical Convergence

Register for the Summit and read more about it here.

NASCIO Annual Conference Set for October

The National Association of State Chief Information Officers is holding its annual Conference October 10th through October 13th in Seattle, Washington. The conference will host several discussion sessions, lectures, and networking opportunities covering emerging technology topics. Read more about the conference and register here.

Federal Advisories Released

CISA, the FBI, and the National Security Agency (NSA) have released a joint Cybersecurity Advisory regarding the increased Conti ransomware threat. Recommended mitigation measures include frequently updating systems and software, requiring multi-factor authentication, and implementing network segmentation. Read the advisory here.

CISA and the NSA also released an information sheet on selecting and hardening virtual private networks (VPNs) – a list of factors for consideration when selecting a network and top recommendations for secure use. Read the guide here, and additional CISA alerts, advisories and news can be found here.

Aspen Institute Releases Set of DEI Priority Approaches

The Aspen Institute has released a set of recommended approaches for achieving better diversity, equity and inclusion in the cybersecurity field following two expert roundtables. The recommendations addressed recruitment and qualification improvement, accountability and advisory partners, and resource sharing. Read the report here.

DOE Roundtable Discussion on Energy Cybersecurity

On **Wednesday, October 6th from 10:00 – 11:00am ET**, Deputy Secretary of Energy David Turk will convene an expert roundtable with federal and industry partners to announce new initiatives addressing the cyber threats facing the nation’s energy grid. Access the livestream here.

Cybersecurity News

Montana State Universities Plan to Adopt Course-Sharing Program

The Montana State University System plans to adopt Quottly, a course-sharing admin platform, to improve access to courses and address workforce needs. Montana is working on a "hub and spoke" system where students take classes at a single institution but pull from other organizations to finish their degrees. Read more about Montana's developments here.

California AG Reminds Medical Industry to Report Ransomware Attacks

In August, California's Attorney General issued a bulletin reminding health care organizations to report data breaches and cyber attacks after multiple ransomware attacks against the health care industry went unreported. California law requires health care providers to report to the AG's office any breach or attack that affects the information of 500 or more patients. Read more about the bulletin here.

Lack of Reporting Requirements an Issue in K-12 Schools

Only a fraction of schools publicly reported cybersecurity incidents in 2021. This article examines Recorded Future's investigation into state ransomware reporting requirements for school districts and found that most states do not have any. Read more about this issue here.

Treasury Department Sanctions Crypto Exchange

As part of an ongoing effort against ransomware threat actors, the Treasury Department's Office of Foreign Assets Control (OFAC) announced sanctions against a virtual currency exchange, Suex. This is the first time a virtual currency exchange has been designated by OFAC. OFAC also released an updated advisory on potential sanctions risks for facilitating ransomware payments. Read more about the designation here and the updated advisory here.

StateRAMP Announces First Publication of Authorized Vendor List

StateRAMP, a nonprofit led by state and local governments to manage third-party supplier cybersecurity risks, has released its first list of vetted and authorized cybersecurity products. Read more about StateRAMP and its initiatives here.

NGA Government Relations Updates

Cyber Provisions Included in the House's NDAA

Several cybersecurity measures were included in H.R. 4350, the National Defense Authorization Act for Fiscal Year 2022 (NDAA). The legislation includes amendments for cyber incident reporting for critical infrastructure and CISA's CyberSentry program. The Senate is working on its own version of the bill, which looks to include increased funding for cybersecurity across the Department of Defense and the development of a joint zero trust strategy within the Department. Read more about the House legislation here and the Senate's bill here.

Senate HSGAC Introduces Cyber Reporting Legislation

Senators Gary Peters (D-MI) and Rob Portman (R-OH) of the Senate Homeland Security and Governmental Affairs Committee (HSGAC) introduced legislation that would require critical infrastructure companies to report cybersecurity incidents to CISA. The legislation comes after testimony from CISA Director Jen Easterly, National Cyber Director Chris Inglis and Federal CISO Chris DeRusha in support of reporting requirements for critical infrastructure organizations. There is potential for the legislation to be attached to the Senate's NDAA bill. Read more about the testimony here and the legislation introduced here.

Secretaries Mayorkas and Raimondo Announce Action to Strengthen Cybersecurity Infrastructure

Secretary of Homeland Security Alejandro Mayorkas and Secretary of Commerce Gina Raimondo released a joint statement on the issuance of preliminary cybersecurity performance goals as directed by President Biden's National Security Memorandum (NSM), "Improving Cybersecurity for Critical Infrastructure Control Systems." The goals are intended to be the first step of the President's NSM objectives to strengthen the cybersecurity of the nation's critical infrastructure control systems. Read the preliminary performance goals and objectives here.