NGA Cybersecurity Newsletter

August 31, 2021
Contact: John Guerriero (jguerriero@nga.org)
202-624-5372

Resource Center Announcements

Introducing Steve Fugelsang – New Program Director, Cybersecurity

Steve joins NGA's Cybersecurity Program from the Aspen Institute's Digital/Cybersecurity Group. Steve previously served as an attorney in the U.S. Army Judge Advocate General's Corps at Ft. Drum, Ft. Meade, and in Afghanistan, as well as in the U.S. Department of Justice National Security Division. Welcome Steve!

NGA Webinar: Cybersecurity for the Water and Wastewater Systems Sector

Please join NGA on **Wednesday, September 22 from 3:00 – 4:00pm ET** for a webinar exploring the cybersecurity landscape of the water and wastewater systems sector. We'll convene a panel featuring national and state experts across the private and public sectors, including Dr. David Travers, Director of the Water Security Division, Office of Water at the U.S. Environmental Protection Agency and Marty Edwards, Vice President of Operational Technology Security at Tenable. Please register for the webinar here.

On August 17th, NGA hosted a webinar on **How SLTT Governments Can Counter Ransomware Attacks** featuring Sherrod DeGrippo, Vice President of Threat Research & Detection at Proofpoint and Thomas Millar, Senior Advisor with CISA's Cybersecurity Division. View the recording here.

Deadline for Applications: GridEx VI National Energy Security Exercise

This is a reminder that the deadline to apply for NGA's GridEx VI exercise technical assistance and state cohort request for applications (RFA) is this **Thursday, September 2, 2021, @ 2:00 PM PT | 5:00 PM ET.** Thank you to those of you who have expressed interest in participating. Please don't hesitate to contact Carl Amritt here if you have any questions or concerns about the opportunity, application process or deadline. View the RFA here.

NGA Memo: Information Campaigns and COVID-19 Vaccine Messaging: Applying Lessons Learned from the 2020 Election

This memorandum explores different state tactics for countering election-related information campaigns to augment COVID-19 vaccine messaging

efforts. It suggests doing so may build better public resilience to false information and restore trust in official sources of information. Find the memo here.

ResCon 2021 Postponed

This year's conference has been postponed until April 2022 due to Covid-19 concerns.

NGA Requests for Information:

1. If your state has established a formal cybersecurity taskforce or commission, how were the body's recommendations presented and implemented?

2. 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

Proofpoint Issues Reports on Risk and Phishing

Proofpoint's annual Human Factor Report examines the three main facets of user risk—vulnerability, attacks, and privilege. The report also found that CAPTCHA technology in cyberattacks received 50 times more clicks in 2020 than in 2019. The report is available here.

Proofpoint also released a new study on the Cost of Phishing with its partner, the Ponemon Institute**.** The report reveals that the costs of phishing attacks have nearly quadrupled over the past six years. Read more here.

Cyberspace Solarium 2021 Implementation Report:

The Cyberspace Solarium Commission released its 2021 Annual Report on Implementation, tracking the Commission's 82 recommendations. 22% of the recommendations have been implemented and nearly 60% are nearing implementation or on track. Read the report here.

CISA Issues Guides & Resources

CISA has issued several guides and resources over the past several weeks. These include:

- Launching the Joint Cyber Defense Collaborative, a collaboration between federal, state, local, tribal, and private-sector partners to

develop and execute whole-nation cybersecurity plans. The coalition looks to create unified objectives and plans, share insights, implement preventative measures, and support joint exercises between all parties.
- Communications and Cyber Resiliency Guide to support public safety agencies and others responsible for communications networks in evaluating and improving resiliency capabilities.
- Cybersecurity Workforce Training Guide to assist future and current federal, state and local staff expand their cybersecurity skills and career options.
- CISA's Information and Communications (ICT) Supply Chain Risk Management Task Force has been extended until July 2023. Read more about the task force here and see the ICT Supply Chain Resource Library here
- A fact sheet to address the rise in ransomware attacks and highlight measures to prevent attacks and protect sensitive and personal information if an attack does occur.

K-12 Cybersecurity Standards Released

The K12 Security Information Exchange (K12 SIX) released its first set of best practices and guidance that aims to establish baseline cyber security procedures for public, private, and charter K-12 schools. The best practices were developed by K-12 IT officials in accordance with current risk management strategies. Read the guidance here.

CYBER.ORG also released guidance to help increase cybersecurity literacy among K-12 students and continue building a cybersecurity talent pipeline. The standards focus around computing systems, digital citizenship and security while also covering the Internet of Things and potential threat actors. Find the learning standards here.

Cybersecurity News

Governor Little Launches Cybersecurity Task Force

Idaho Governor Brad Little created a Cybersecurity Task Force that will look to further the state's strategic cyber priorities. The task force will offer recommendations to the governor on ways to bolster the cyber posture of the state government, private sector and citizens. The task force will also have a special focus on election security and cyber workforce development. Read more about the task force here and its first meeting, which focused on workforce development, here.

States Consider Banning Ransomware Payments

New York, Pennsylvania, and North Carolina are considering legislation that would ban state and local government agencies from paying ransom. While these actions possibly may deter future ransomware attacks, there

is debate whether any such actions are overly punitive towards the victim instead of the attacker. Read more here.

Rising Cost of Ransomware Affects Cyber Insurance Rates

C-Suite executives at both AIG and Chubb stated recently that their companies were charging members more based on the rising rate of ransomware attacks. Ransomware now accounts for 75% of all cyber insurance claims, and member premiums are unable to keep up with the increased cost. Impacts of the crisis may include even higher premiums, limited coverage, or even insurance providers exiting the market. Read more about the concerns here.

Vulnerability Discovered in Microsoft's Azure Cosmos Database

A misconfiguration vulnerability in Microsoft's Azure Cosmos Database potentially exposed customer data. While the vulnerability appears to have been remediated, Microsoft and CISA recommend users roll and regenerate their certificate keys. Read Microsoft's guidance on securing access to data in the Azure Cosmos Database here.

K-12 Cyber Incidents Expected to Rise by 86%

The Center for Internet Security (CIS) predicts that attacks will rise by 86% over the next year based on data from academic institutions. Read more here.

Wisconsin Adopts New Insurance Cybersecurity Law

In July, Wisconsin adopted the National Association of Insurance Commissioners' model cybersecurity law. Entities licensed by the Wisconsin Office of the Commissioner of Insurance, including insurers and agents, must adopt investigation procedures, data security program standards, and notification requirements. Unless exempt, licensees must develop and implement a security program that contains physical, technical, and administrative safeguards to protect sensitive and nonpublic information. Read more about Wisconsin's actions here, and find the original legislation here.

NGA Government Relations Updates

$1 Billion in Cyber Grants Outlined in Senate Infrastructure Deal

The Senate passed the Infrastructure Investment and Jobs Act (IIJA). The $1.2 trillion infrastructure package includes key cyber provisions for state and local governments, including a $1 billion dedicated grant program for improving state, local, tribal and territorial (SLTT) government cybersecurity, $100 million for a CISA cyber response and recovery fund, and $35 million for CISA to establish oversight over government critical infrastructure. NGA previously worked with other SLTT

organizations to advocate for this program and funding. Read NGA's commentary on the package here.

White House and Industry Leaders Announce Cybersecurity Initiatives

President Biden met with key stakeholders across the private sector and education field regarding efforts to better support a whole-of-nation cybersecurity posture. Outcomes from the meeting include:

- The National Institute of Standards and Technology (NIST) will work with industry to create a framework to strengthen the security of the technology supply chain;
- Expansion of the Industrial Control Systems Cybersecurity Initiative to include natural gas pipelines;
- Pledges from private companies and other organizations to improve supply chain security and increase cyber education and training efforts and initiatives.

Read more about the meeting here.

Senators Introduce Legislation to Fight Cybercrime and Protect Against Online Attacks

Senators Brian Schatz (D-HI), John Cornyn (R-TX), Thom Tillis (R-NC), and Richard Blumenthal (D-CT) introduced the Better Cybercrime Metrics Act, which seeks to improve data collection on cybercrimes. The bill would encourage local and federal law enforcement agencies to report cyberattacks to the FBI and require the FBI to report metrics on cyber crime as it does for other types of property crime. The bill also would authorize a study on creating a common language around cyber crimes and the incorporation of cyber-related questions into the annual National Crime Victimization Survey. Read more about the legislation here.