NGA Cybersecurity Newsletter

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

Resource Center Announcements

Five States Join NGA for Policy Academy on State Cybersecurity

NGA is pleased to announce that five states will join the 2021 NGA Policy Academy to Advance Whole-of-State Cybersecurity. After a very competitive application process, NGA will be working with Indiana, Kansas, Missouri, Montana and Washington to develop action plans to improve their respective cybersecurity priorities. Thank you to all the states who submitted applications. You can read more about the Policy Academy here and can see NGA's announcement here.

Upcoming NGA Webinar on GridEx VI: March 31st @ 3:30pm ET

NGA and the National Association of Regulatory Utility Commissioners (NARUC) are hosting a webinar about state participation in GridEx VI, the biennial energy security exercise hosted by the North American Electric Reliability Corporation (NERC). The webinar will occur on **Wednesday, March 31, 2021, from 3:30-4:30 PM ET**. Participants will learn about this national energy security exercise and its focus, how states can participate and will hear from two state representatives that participated in GridEx V.

Featured speakers:

- Kate Ledesma, Resilience and Policy Coordination Manager, Electricity Information Sharing and Analysis Center, North American Electric Reliability Corporation
- Dan Searfoorce, Reliability and Emergency Preparedness Supervisor, Pennsylvania Public Utilities Commission
- Jimmie Collins, Senior Planner, Hawai'i Office of Homeland Security

Please register for the webinar here.

NGA Request for Information:

1. How is your organization looking to promote a culture of diversity, equity, and inclusion in its cybersecurity workforce?

2. If your state conducts risk assessments and incident response services for local governments, what role do data and metrics play in performance improvement and budget requests?

3. Vendor contracts: does your state use a vetted vendor list or adopted a standard language for contracts?

   Please reach out to John Guerriero here on the above requests.

Cybersecurity Resources

Rise in Phishing Attacks Using Fake Vaccine Websites

Palo Alto Networks released a report finding that since vaccine distribution began a few months ago, there has been a major increase in scams attempting to steal personal data by posing as websites offering vaccines or appointments. Read the report here.

NIST Releases a Draft Cybersecurity Framework Profile for Election Infrastructure

NIST, in collaboration with the MITRE Corporation, developed a draft cybersecurity framework profile for voting equipment and information systems supporting elections. The profile is designed to support both elections and IT officials by offering a voluntary, supplemental risk-based approach to reduce cyber risk to elections infrastructure. NIST encourages the public to submit comments by May 14th. Read more about the profile here.

NCCoE Releases Draft Version of Mobile Device Security Guide

The National Cybersecurity Center of Excellence (NCCoE) released a draft version of the NIST Cybersecurity Practice Guide SP 1800-22, *Mobile Device Security: Bring Your Own Device (BYOD).* The guide looks to help provide a framework to help organizations in setting security standards for use of personal mobile devices in work-related activities. NCCoE is encouraging public feedback on the draft by May 3, 2021. Read the guide here.

DOL Issues Fact Sheet on Cybersecurity Apprenticeship Programs

The U.S. Department of Labor released a snapshot for cybersecurity apprenticeship programs, including snippets on challenges facing the industry, occupations available for apprenticeship programs, and ways apprenticeship programs benefit both organizations and participants. Read the guide here.

State of K-12 Cybersecurity Year in Review

The K-12 Cybersecurity Resource Center and the K12 Security Information Exchange (K12 Six) published a report reviewing an unprecedented year in K-12 cybersecurity. According to the report, the number of publicly disclosed cybersecurity incidents affecting the K-12 community increased by 18% from 2019, and 2020 marked the highest number of incidents (408) since the K-12 Cybersecurity Resource Center began tracking in 2016. Read the report here.

Upcoming NICE Webinar: Getting Girls into Cybersecurity Careers

NICE is holding a webinar from 2:00 – 3:00pm ET on April 21 on Getting Girls into STEM and Cybersecurity – Pathways to Progress. The webinar will explore ways communities can encourage girls to join the field and make them feel welcome once there. Register for the webinar here.

Cybersecurity News

Microsoft Exchange Server Vulnerabilities Exploited

Several zero-day vulnerabilities in Microsoft Exchange Server software are actively being exploited by a Chinese-sponsored threat group and other malicious actors. Delays in patching has led to increased exploitation of the vulnerability. Microsoft has released out-of-band security updates to address the vulnerabilities and CISA issued several directives and alerts, including:

- Emergency Directive 21-02: Mitigate Microsoft Exchange On-Premises Product Vulnerabilities
- Alert AA21-062A: Mitigate Microsoft Exchange Server Vulnerabilities

CISA **recommends** the following actions: 1) ensure all professionals responsible for securing the state's IT infrastructure mitigate and remediate potential damage, and 2) amplifying both the severity of the threat and next steps for local governments, critical infrastructure partners and businesses throughout the state. Read more here.

CISA and FBI Warning for Spear-Phishing Campaign

The FBI and CISA released a joint advisory on a new spear-phishing campaign, Trickbot. The campaign uses malicious emails that claim to have proof of a traffic violation. Read more here.

IRS Warns of Tax-themed Phishing Scams Against .Edu Addresses

The IRS recently issued an advisory regarding an email scam operation that impersonates emails from the IRS targeting educational institutions, especially those with a .edu email address. The scam emails displays the IRS logo and looks to lure victims with the phrase “tax refund payment” in the subject line. Read the advisory here.

Biden Administration Prepares EO on Cybersecurity

A planned executive order from the Biden administration would establish a requirement for software vendors to disclose cybersecurity breaches to their federal government customers. The order would also look to implement cybersecurity controls within federal agencies, such as multi-factor authentication and data encryption, and require vendors to enhance their digital preservation and work with CISA on incident response. Read more here.

Michigan Launches App to Protect Mobile Devices

The state of Michigan is offering its residents access to the Michigan Secure app – a free application that detect threats to their mobile devices. The app alerts users of suspicious activity, including warnings about unsecured Wi-Fi and conducts threat scans of other apps. The app does not collect, store or monitor personal data. Read more here.

Safe Harbor Bill in Connecticut Legislature

The Connecticut General Assembly is considering a bill that looks to encourage voluntary adoption of cybersecurity best practices and provide a safe harbor for organizations that put in place reasonable cyber controls, such as the NIST framework or the CIS Controls. Read more here.

CIS Providing MDBR to Hospitals for Free

In response to the wave of ransomware attacks targeting the healthcare sector during the COVID-19 pandemic, the Center for Internet Security (CIS) is offering Malicious Domain Blocking and Reporting (MDBR) service at no cost to public and private hospitals and healthcare organizations across the country. Read more here.

Ransomware Actors Publish Data Stolen from Universities

Data stolen from several universities has been posted to a leak site associated with Clop, a new ransomware group. Impacted schools include the University of California, Merced, University of Maryland, Baltimore, the University of Colorado and the University of Miami, as fallout continues from the Accellion breach. Read more here.

Dot Gov Domain Transferring to CISA

CISA announced that in April, it will start overseeing the .gov top-level domain. The domain was previously under the oversight of the U.S. General Services Administration until the DOTGOV Act of 2020 shifted responsibility. Read more here.

NGA Government Relations Updates

DHS Releases TVTP Notice of Funding Opportunity

DHS recently issued a notice of funding opportunity (NOFO) for its 2021 Targeted Violence and Terrorism Prevention (TVTP) Grant Program for SLTT entities, nonprofits, and institutions of higher education. The FY21 program establishes priorities in:

- Preventing Domestic Violent Extremism
- Enhancing Local Threat Assessment and Management Capabilities
- Implementing Innovative Solutions for Preventing Targeted Violence and Terrorism
- Challenging Online Violence Mobilization Narratives

Applications are due May 25, 2021. Read the NOFO here.

Bill Aims to Assist National Science Foundation on Cybersecurity

The House Science Committee recently introduced the National Science Foundation for the Future Act that would increase funding for the National Science Foundation to help increase efforts in cybersecurity and emerging technology challenges. Read more here.