NGA Cybersecurity Newsletter

October 16, 2019
Contact: John Guerriero (jguerriero@nga.org)
202-624-5372

October is National Cybersecurity Awareness Month (NCSAM)! As your state plans any upcoming events or awareness campaigns, please feel free to send any news and information to John Guerriero at jguerriero@nga.org.

Resource Center Announcements

Introducing Khristal Thomas – New Policy Analyst, Cybersecurity, Technology & Communications

Khristal joins NGA's Homeland Security and Public Safety Division from the Center for Strategic and International Studies' (CSIS) Technology Program, where she was a research intern. Khristal is obtaining her Master's in technology policy at George Mason. While in school, she also interned at BSA and VMware—and has prior consulting experience from Oracle. Welcome Khristal!

October Resource Center Webinar

Ransomware and the Role of MS-ISAC: October 28th at 3:00pm ET

Please join us for the next Resource Center webinar to discuss strategies states can take to mitigate the risks associated with ransomware, the critical role MS-ISAC plays in the cybersecurity landscape, and how local and state governments can best engage in information sharing.

Brian Calkin, CTO for the Center for Internet Security, will cover best practices for recovery, cyber hygiene tasks organizations can invest in and how stakeholders can leverage MS-ISAC to counter the risks associated with ransomware attacks.

Please feel free to share this with any state and local partner. Contact Khristal Thomas (kthomas@nga.org) if you have any questions.

2019 National Cybersecurity Awareness Month Toolkit and Proclamation Released

October is National Cybersecurity Awareness Month, and this year's theme is to "OWN IT. SECURE IT. PROTECT IT." You can access the toolkit released by CISA and National Cyber Security Alliance (NCSA) here. The list of NCSAM events can be accessed here.

Additionally, CISA and the MS-ISAC recently distributed the NCSAM 2019 Proclamation to every Governor and CISO's office across the country to increase local level cyber outreach and awareness. Please feel free to share the proclamation with your jurisdictions for their sign-on.

NGA Information Requests:

1. Is your state providing misinformation and disinformation guidance to political campaigns? If your state has advice or custom tools that it provides, please reach out to John Guerriero here.

2. How is your state using DHS's Homeland Security Grant Program (HSGP) funds for cybersecurity? Do you currently have a statewide program for the benefit of local entities? If you have already launched projects, what promising practices and lessons learned can you share? Please reach out to Maggie Brunner here.

3. Is your state using HAVA funds to pay for state active duty hours for National Guard to enhance cybersecurity? If so, please feel free to reach out to Maggie Brunner here.

Cybersecurity Resources:

Advancing Cybersecurity at Scale in the Cloud

With U.S. federal agencies obtaining more funding to spend on cloud advancements, Google Cloud released a whitepaper outlining several security considerations that agencies should keep in mind when exploring transitions. These include engaging providers that have implemented strict security measures, leveraging AI and machine learning to bolster security, and increasing visibility and transparency in a system by centralizing cloud infrastructure.

Report Shows that Hackers Targeted 17 Organizations in the U.S. Utilities Sector

A Proofpoint report shows that hackers likely associated with the Chinese government conducted phishing attempts against 17 entities in the U.S. utilities sector from April through August 2019. According to the report, the attacks will likely continue to ramp up against the sector as techniques continue to become more sophisticated.

A Federal Backstop for Insuring Against Cyberattacks?

This Brookings report explores past involvement by the U.S. government in the insurance field when acts of war and/or terrorism occur and explores what that may look like for cyber incidents.

Mark Your Calendars:

October 22: Operational Collaboration in Cyberspace: Beyond Information Sharing

Attacks on Atlanta, Baltimore, Louisiana, Florida, Texas show how, on the eve of the 2020 elections, cyber adversaries are broadening their reach and targeting an increasingly diverse array of victims. Yet efforts to improve public-private coordination in cybersecurity often focus on the relationship between federal agencies and Fortune 500 firms. Countering our most sophisticated adversaries demands that government and industry reimagine joint cyber defense efforts with the full spectrum of stakeholders: local, state, federal, and private.

Please join the Aspen Institute's Cyber & Technology Program and the National Governors Association on **Tuesday, October 22, 2019** from **10:30 a.m. to 12:00 p.m.** for a conversation about how stakeholders can combine their operational capabilities and authorities to impose strategic costs on cyber adversaries. The discussion will feature the Assistant Director for Cybersecurity of CISA, **Jeanette Manfra**, Chief Information Security Officer for the Commonwealth of Pennsylvania **Erik Avakian,** President & CEO of the Cyber Threat Alliance **Michael Daniel**, and **Angelina Panettieri**, Principal Associate for Technology and Communications for the National League of Cities. The conversation will be moderated by **Maggie Brunner,** Program Director, Homeland Security & Public Safety Division at the National Governors Association.

Space is limited, so please register here to reserve your seat.

Registration Opens for GirlsGoCyberStart

The GirlsGoCyberStart program is available in 2020. Interested states should contact Alan Paller (apaller@sans.org). As gubernatorial support of the program has historically increased states' student participation significantly, NGA can provide governors' offices with additional information. Email John Guerriero at jguerriero@nga.org for more details.

November 18-20: NICE 2019 Conference and Expo

The annual NICE Conference and Expo brings together thought leaders from industry, government, academia and non-profit organizations to address cybersecurity education, training and workforce needs. The theme of this year's conference in Phoenix, Arizona is *Reimagining the Future of the Cybersecurity Workforce: Adapting to a Changing Landscape*.

Cyber News

NSA Launches New Cyber Defense Directorate

The National Security Agency launched an organization to prevent cyberattacks on sensitive government and defense-industry computers – with an eye also toward helping shield critical private-sector systems. In this organization, the NSA will join under one roof threat detection, cyber defense and future-technologies personnel. Read more about the Cyber Defense Directorate here.

Ohio House Lawmakers Approve Civilian Cyber Reserve

The Ohio House voted unanimously on Senate Bill 52 which creates a civilian cyberforce within the Ohio National Guard to respond to cyberattacks against election systems, governments, businesses, and critical infrastructure. The bill returns to the Senate, where it passed unanimously earlier this year. Some of the bill's requirements include that post-election audits be conducted in at least three local races each year and that the Secretary of State's office hires a chief information security officer to work with county boards of elections. Read more here.

Senate Intelligence Report Warns that Russia's Activity in 2016 Offers Preview of Election Interference in 2020

The Senate Intelligence Committee released a bipartisan report warning that Russian efforts to influence the 2016 presential election may grow and evolve while inspiring other actors to make similar efforts in 2020. The second in a series investigating Russian interference in the 2016 election, the report concludes that Russian social media disinformation operations, especially by the Kremlin-linked Internet Research Agency, were voluminous, fast, and wide-ranging across a number of platforms. The committee makes several recommendations, including calling on social media companies to increase information sharing with the public and private sectors and to develop methods to notify users subjected to online disinformation. Read the full report here.

Cyber Storm 2020 Could be DHS' Most Rigorous Drill for Critical Infrastructure Yet

DHS officials are planning Cyber Storm 2020, the agency's bi-annual exercise designed to test critical infrastructure companies' response capability to cyber-attacks. The exercise, planned for Spring 2020, will focus on critical infrastructure interdependence and how state and local officials can collaborate with DHS on incident recovery. Read more on the plans for the exercise here.

Cybersecurity Apprenticeship Programs Expand in New York and Florida

New York Governor Andrew Cuomo announced a $3 million investment in The State University of New York's Apprenticeship Program. The funding will expand apprenticeship programs in cybersecurity, artificial intelligence, and information technology as well as other growth industries.

The U.S. Department of Labor awarded Florida International University (FIU) $2 million to develop the Cybersecurity Apprenticeship Program. The initiative aims to train 800 apprentices over a four-year period in critical cybersecurity skills. FIU will also collaborate with The Coalition of Urban Serving Universities to scale and replicate the model at other institutions.

Free Federal Program Helps Local Governments Beef up Cybersecurity

A team within the Department of Homeland Security is helping governments at all levels better secure their systems. The DHS Cybersecurity Assessments program offers its services free of charge to any organization that requests them. Services are provided both remotely and with in-person technical support to identify and analyze system vulnerabilities. The program includes cyber hygiene assessments, phishing campaign assessments, and remote penetration testing. Read more about the program here.

Microsoft Offering Windows 7 for Free in Support of Election Officials for 2020

Microsoft announced that it will offer state and local election officials free security support for Windows 7 operating systems used in voting systems through 2020.

Governors Highlight Importance of Collaboration on Cybersecurity and Election Security

At the seventh annual Wisconsin Governor's Cybersecurity Summit, Governor Tony Evers highlighted the importance of state and local leaders, businesses, and educational institutions working together to prevent and respond to cyber incidents. The summit brought together leaders from the public and private sectors to share information and best practices for improving the security of state and local networks and election infrastructure.

Led by the Minnesota Secretary of State and Governor Tim Walz's office, state lawmakers, election workers, and government officials convened for a two-day workshop dedicated to designing a state-wide election cybersecurity plan for 2020. Governor Walz and Secretary of State Steve Simon both spoke on the importance of state and local collaboration to secure the integrity of the election system.

Updates from NGA Advocacy

The Senate Appropriations Committee on Homeland Security approved its fiscal year 2020 funding bill, providing $70.7 billion for the Department of Homeland Security. The bill provides CISA $2 billion to increase state and locality funding. The bill also includes $17.8 billion for the Disaster Relief Fund and $2.7 billion for grant funding under the Federal Emergency Management Agency (FEMA).

The U.S. Senate has approved new legislation aimed at helping government agencies and private-sector companies combat ransomware attacks. The legislation comes as local governments and schools continue to be hit by sophisticated – and in some cases, coordinated – ransomware attacks. The proposed law, the "DHS Cyber Hunt and Incident Response Teams Act," authorized DHS to invest in and develop "incident response teams" to help organizations battle ransomware attacks. Read more here.

NGA Resource Center for State Cybersecurity Sponsors

- American Electric Power
- Anomoli
- AT&T
- Deloitte
- Google
- Proofpoint
- Rapid7
- Splunk
- Symantec
- Tenable
- VMware