NGA Cybersecurity Newsletter

December 19, 2019
Contact: John Guerriero (jguerriero@nga.org)
202-624-5372

Resource Center Announcements

Resource Center Webinars

COOP & COG Plans: January 27, 2020

Please join us **Monday, January 27 from 3-4pm Eastern** for the next Resource Center webinar on COOP and COG plans. Please also keep an eye out for NGA's schedule of 2020 webinars.

Contact Khristal Thomas (kthomas@nga.org) if you have any questions.

November Webinar on Cyber Insurance
During our November webinar, Alan Shark, the Executive Director of the Public Technology Institute (PTI), addressed what state and local governments should look for in a cyber insurance policy, what is typically covered in a cyber insurance policy and share best practices for state and local governments. Slides (PDF) and a recording (MP4) are available.

NGA Information Requests:

1. 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.

2. What is your state National Guard's parameters for supporting election cybersecurity? If you would like to share more about your Guard's current efforts, please feel free to reach out to Maggie Brunner here.

3. How is your state funding cyber forensic capabilities? If you have a creative approach or promising practice, please reach out to Maggie Brunner here.

4. How is your state incentivizing or supporting government agencies and businesses in your jurisdiction to adopt the NICE framework? Please reach out to John Guerriero with promising practices here.

Engagement Opportunities

NIST Request for Information

The NICE Cybersecurity Workforce Framework (NIST SP 800-181) is a reference resource that assists employers in the public and private sectors to align descriptions of the roles, tasks, and relevant knowledge, skills and abilities included in cybersecurity work. NICE is planning an update to this important framework as well as a new resource website. NIST is especially interested in making improvements to the NICE Framework that will encourage and increase adoption by the private sector so any input on how to make it more relevant to and usable by employers is welcome. Please submit feedback here by **January 13, 2020**.

Cybersecurity Resources:

NIAC Calls Cyber Threats to Critical Infrastructure an "Existential Threat"

The National Infrastructure Advisory Council (NIAC) published a draft report addressed to President Trump stating that cyber threats to critical infrastructure pose an "existential threat" to national security. The report calls for the Trump Administration to establish a Critical Infrastructure Command Center to facilitate the sharing of classified information between government agencies and companies at risk of cyberattack. It also proposes the creation of an independent Federal Cybersecurity Commission to mitigate cyber risks to critical infrastructure whose disruption would severely impact national security. Read the draft report here.

Brennan Center Releases Report on Election Security

In a recent report, the Brennan Center provides guidance for election officials on ways to safeguard against Election Day disruptions. The report offers a communication strategy and recommendations for preventing and recovering from the failure of four critical systems: e-poll books, voting machines, voter registration databases, and election night reporting systems. Read the full report here.

Global Cyber Alliance Launches Program to Bolster Election Cybersecurity Efforts

Global Cyber Alliance (GCA) announced the launch of the Craig Newmark Trustworthy Internet and Democracy Program, which will provide free toolkits and online forums on cybersecurity to news outlets, election officials, community organizations, and government offices. Read more here.

NGA Joins the National Association of Secretaries of State (NASS) in Supporting #TrustedInfo2020

NASS has launched a bipartisan education effort aimed at promoting state and local election officials as the trusted sources of election information. #TrustedInfo2020 aims to reduce the misinformation and disinformation surrounding elections by directing voters directly to election officials' websites and social media pages. NGA joins a host of other organizations in supporting NASS in this effort.

Girls Go CyberStart Sees Over 2,650 Students Registered with 44 Days Remaining

Over 2,650 students have completed registration for Girls Go Cyberstart. In just the first three days of registration, over 1,000 students and 300 teachers registered. Girls Go CyberStart is an interactive, online program designed to engage high school-aged girls and promote cyber career opportunities. The top three states leading the registration scoreboard are: Texas, with 479 students registered; New Jersey, with 328 students registered; and Nevada, with 164 students registered. Read more and register here.

Cyber News

NIAC Calls Cyber Threats to Critical Infrastructure an "Existential Threat"

The National Infrastructure Advisory Council (NIAC) published a draft report addressed to President Trump stating that cyber threats to critical infrastructure pose an "existential threat" to national security. The report calls for the Trump Administration to establish a Critical Infrastructure Command Center to facilitate the sharing of classified information between government agencies and companies at risk of cyberattack. It also proposes the creation of an independent Federal Cybersecurity Commission to mitigate cyber risks to critical infrastructure whose disruption would severely impact national security. Read the draft report here.

Congress to Review Trump Administration Offensive Cyber Policy

Lawmakers won the right to review the Trump administration's new offensive cyber policy after a lengthy battle. Rep. Jim Langevin (D-RI) led the bipartisan charge to insert a provision into the defense policy bill allowing Congress to review the National Security Presidential Memorandum 13. Read more here.

FCC Vote on Chinese Telecommunications Giants Huawei and ZTE

On November 22, the Federal Communications Commission (FCC) voted to block broadband subsidies to companies that use telecommunications equipment from Chinese companies Huawei and ZTE – effectively pushing the companies entirely out of American telecommunications networks. Read more here.

Governor Edwards Declares Cyberattack Emergency

In late November, Louisiana Governor John Bel Edwards declared a state of emergency following a ransomware attack on state government servers. The declaration enabled the Office of Motor Vehicles, Department of Transportation and Development, and the Department of Revenue to take necessary actions, including waiving fees and fines, to assist members of the public in the wake of the attack. Read more here.

5G Fund for Rural America Announced

The FCC announced the establishment of the 5G Fund, which will make close to $9 billion in Universal Service Fund support available to carriers for the deployment of advanced 5G mobile wireless services in rural America. The 5G fund will replace the Mobility Fund Phase II, which was aimed at providing 4G LTE service to unserved areas, due to the unreliable coverage data submitted by providers that would have been used to target the funds.

The funds will be allocated through a reverse auction and will target areas that are hard-to-serve with sparse populations or rugged terrain. Read the press release here.

NGA Government Relations Updates

S.333 – National Cybersecurity Preparedness Consortium Act of 2019

The Senate passed S.333, which would authorize the DHS to collaborate with the National Cybersecurity Preparedness Consortium to conduct cybersecurity training and research. Read the full text of the bill here.

S.1846 – State and Local Government Cybersecurity Act of 2019

The Senate passed S.1846, which would encourage information sharing between the DHS' National Cybersecurity and Communications Integration Center and the Multi-State Information Sharing and Analysis Center. Read the full text of the bill here.

H.R. 5394 – Strengthening State and Local Cybersecurity Defenses Act

H.R. 5394 was introduced in the House by Rep. Van Taylor (R-TX), which would require the Critical Infrastructure Security Agency (CISA) to offer more outreach and support to state and local governments. Several of the bill's requirements include pushing CISA to conduct exercises and trainings for local governments, assist with threat-sharing, and help state and local governments craft vulnerability disclosure policies. Read the full text of the bill here.

DHS Appropriations Bill Released

Appropriations are listed as follows:

Homeland Security:

- Border Wall Construction: **$1.25B**
- FEMA Grants: **$2.89B**
  - State Homeland Security Grant Program: **$560M**
  - Urban Area Security Initiative: **$665M**
  - Emergency Management Performance Grants: **$355M**
  - Flood Hazard Mapping & Risk Analysis: **$263M**
- Disaster Relief Fund (DRF): **$17.8B**
- CISA: **$2B**
  - Cybersecurity Education and Training Assistance Programs: **$4.3M**
  - Continuous Diagnostics and Mitigation Program: **$3.6M**

Elections:

- Election Assistance Commission Grants: **$425M**
- Election Infrastructure Security Initiative under CISA: **$43.5M**

NGA Resource Center for State Cybersecurity Partners

Commented [JG1]: May need another review from last month if anything changed

- American Electric Power
- Anomali
- AT&T

- CompTIA
- Deloitte
- Google Cloud
- Proofpoint
- Rapid7
- Raytheon
- Splunk
- Symantec
- Tenable
- VMware