

# NGA Cybersecurity Newsletter

January 30, 2020

Contact: John Guerriero ([jguerriero@nga.org](mailto:jguerriero@nga.org))

202-624-5372

---

## Resource Center Announcements

### **NGA-NASCIO Joint Publication on State and Local Partnerships**

In collaboration with the National Association of State Chief Information Officers, NGA recently released “Stronger Together: State and Local Cybersecurity Collaboration.” This publication outlines promising programs that states have initiated to enhance collaboration with their local government counterparts for cyber resilience. It also provides high-level recommendations for state officials looking to strengthen partnerships with local government officials on cybersecurity. Read more [here](#).

### **Resource Center Webinars**

#### **State Highlight: Indiana Emergency Manager Cybersecurity Toolkit for Locals: February 24, 2020**

Please join us **Monday, February 24 from 3-4pm Eastern** for the next Resource Center webinar highlighting the *Indiana Emergency Manager Cybersecurity Toolkit*. Chetrice Mosley, the Cybersecurity Program Director for the State of Indiana, will join to walk through the toolkit, discuss the role of emergency management in cybersecurity planning and response, and offer recommendations for other states looking to create similar resources. To download the toolkit and access other resources for emergency managers, click [here](#). Please also keep an eye out for NGA’s schedule of 2020 webinars.

Please register for the webinar [here](#), and contact Khristal Thomas [here](#) 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 cyber insurance policies, what is typically covered in cyber insurance policies and shared best practices for state and local governments. Slides ([PDF](#)) and a recording ([MP4](#)) are available.

## **NGA Information Requests:**

1. How is your state consolidating and disseminating threat intelligence to localities? Does your state's SOC and Fusion Center categorize different security threats? Please reach out to John Guerriero [here](#).
2. How is your state funding cyber forensic capabilities? If you have a creative approach or promising practice, please reach out to Maggie Brunner [here](#).
3. How is your state using DHS's Homeland Security Grant Program (HSGP) funds for cybersecurity? If you have already launched projects, what promising practices and lessons learned can you share? Please reach out to Maggie Brunner [here](#).
4. 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](#).
5. 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](#).

---

## Cybersecurity Resources

### **NASCIO Report Explores the Future Role of the State CIO**

NASCIO and Accenture present the results of a joint research project examining what role state CIOs will play going forward as well as opportunities for the position to drive state innovation. Read more [here](#).

### **NIST Releases Privacy Framework and Draft Guidelines for Businesses to Defend Against Ransomware**

The National Institute of Standards and Technology (NIST) recently released a privacy framework, a voluntary tool designed to help organizations identify and manage privacy risk. Read more about the framework [here](#).

NIST and the National Cybersecurity Center of Excellence (NCCoE) also released for public comment a draft guide on defending against ransomware. The guide aims to assist private sector executives, CISOs, and system administrators detect and respond to data integrity events,

including ransomware. The [public comment period](#) closes on February 26, 2020. Read the full guide [here](#).

### **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](#).

### **CISA Releases Insights on Increased Geopolitical Threats and Tensions**

With the recent heightened tension with Iran, CISA released a list of threat factors to be on the look out for as well as precautionary steps your organization can take to bolster both its physical and cybersecurity. Read the release [here](#).

### **Addressing the Cybersecurity Workforce Gap**

The Center for Strategic and International Studies (CSIS) released a report examining the cybersecurity workforce gap, offering recommendations for policymakers, educators, and employers. Recommendations include supporting quick, intensive training programs to reskill workers into cybersecurity careers, emphasizing soft skills in learning environments, and building relationships between education organizations and industry to communicate critical workforce needs and skills gaps. Read the full report [here](#).

### **Election Security Resources Released**

#### **Belfer Center Elections Battle Staff Playbook**

The Belfer Center’s Defending Digital Democracy Project (D3P) released its new manual, The Elections Battle Staff Playbook, to provide state and local elections officials guidance on how to build their operations teams and tools to identify issues. The manual offers recommendations for officials on staffing strategy, communication plans, incident management and tracking, and much more. Read the manual [here](#).

### **Brennan Center Guidance for Election Officials**

The Brennan Center for Justice at New York University Law School provided 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](#).

### **GCA Launches Program Supporting Election Officials**

The 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 Supports #TrustedInfo2020**

NGA joins the National Association of Secretaries of State (NASS) in supporting [#TrustedInfo2020](#). The bipartisan education effort is 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.

---

## Cybersecurity News

### **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](#).

### **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](#).

## **State Cybersecurity News**

### **New Maryland Bill would Criminalize Ransomware Possession**

The Maryland Senate recently [introduced](#) a bill that would make possession of ransomware a misdemeanor and punishable by up to 10 years in prison. Other states, including Michigan, Wyoming and California, have passed similar legislation. Given the often anonymous nature of cybercrime, legal frameworks are only a component of a more comprehensive protection plan, ideally complemented by exercised response plans and coordination between state, local and federal stakeholders and the private sector.

### **Louisiana Governor Discusses Cybersecurity Defense in Second Inaugural Address**

In his [Second Inaugural Address](#), Louisiana Governor John Bel Edwards stressed the need for cybersecurity preparedness in the state while highlighting the [LA Cybersecurity Commission's](#) work in supporting the state's cybersecurity defense.

In late November, Governor 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](#).

### **North Dakota Building a Shared Infrastructure**

North Dakota's IT Department is looking to build a cross-state shared security operations center that has the capability to adapt to different threats and provide resources and intelligence to those who need it. Read more [here](#).

### **Virginia Increases Election Security Posture**

Virginia's State Board of Elections is looking to implement new voting equipment policies, including upgrading localities to equipment version standards and requirements for electronic poll books. Read more [here](#).

### **South Carolina Governor Approves Funding for National Guard Cybersecurity Facility**

South Carolina Governor Henry McMaster recently released an executive budget that includes funding for the SC National Guard to construct a new DreamPort Cybersecurity Collaborative facility at the University of South Carolina Aiken. The facility will increase the state's cyber response capabilities, providing both classified and unclassified environments while leveraging the state's National Guard's cybersecurity expertise. Read more about the plans for the facility [here](#).

## **Cyber Workforce Development News**

### **Michigan Announces New Job Training Initiative for Veterans**

Michigan Gov. Gretchen Whitmer [announced](#) plans for the expansion of the Cisco CyberVets Scholarship program into Michigan. The program provides free online cybersecurity training and certification to veterans, transitioning service members, National Guard members, Reservists, and military spouses, while also offering free online access to highly sought-after courses in secure infrastructure and cybersecurity operations.

### **Idaho Continues Partnerships Helping Students Explore Cybersecurity Careers**

Idaho Governor Brad Little [announced](#) that the state will continue its partnership with the SANS Institute to assist high school and college students explore cybersecurity careers through the [Girls Go Cyberstart](#) and [Cyber FastTrack](#) initiatives.

### **Girls Go CyberStart Sees Over 10,000 Students Registered with 16 Days Remaining**

Over 10,000 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 three states atop the [registration leaderboard](#) are: Texas, with 1,538 students registered; New Jersey, with 1,006 students registered; and California, with 610 students registered. Read more and register [here](#).

## **NGA Government Relations Updates**

### **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. 4355 – Identifying Outputs of Generative Adversarial Networks Act**

H.R. 4355, which was received by the Senate, would direct the National Science Foundation (NSF) and the National Institute of Standards and Technology (NIST) to support research on generative adversarial networks, i.e., a software system trained to generate artificial outputs (e.g., deepfakes) from authentic inputs (e.g., photographs). Read the full text of the bill [here](#).

### **H.R. 5679 – CISA Director Reform Act**

H.R. 5679 was introduced to the House by Rep. John Katko (R-NY) and would limit to five years the term of the Director of CISA. Read the full text of the bill [here](#).

### **H.R. 5680 – Cybersecurity Vulnerability Identification and Notification Act of 2020**

H.R. 5680 was introduced to the House by Rep. James Langevin (D-RI) and would ensure that CISA has the necessary legal tools to notify entities at risk of cybersecurity vulnerabilities in the enterprise devices or systems that control critical assets of the U.S. Read the full text of the bill [here](#).

### **H.R. 5707 – To Amend the Help America Vote Act of 2002**

[H.R. 5707](#), which was introduced in the House by Rep. Rodney Davis (R-IL), would amend HAVA to direct the Election Assistance Commission to adopt voluntary guidelines for the use of nonvoting election technology. The proposed bill would also establish an Election Cyber Assistance Unit in the Election Assistance Commission.

### **FY 2020 DHS Appropriations Bill Passed**

The appropriations are listed as follows:

Homeland Security:

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

- American Electric Power
- AT&T
- CompTIA
- Deloitte
- Google Cloud
- Proofpoint
- Rapid7
- Splunk
- Tenable
- VMware