NGA Cybersecurity Newsletter

July 23, 2020
Contact: John Guerriero (jguerriero@nga.org)
202-624-5372

Resource Center Announcements

NGA Launches Governors' Election Cybersecurity Action Network (GECAN)

NGA recently obtained grant funding to continue and expand its work on election security. NGA will support governors and their advisors on election issues ranging from cybersecurity, security and resilience, ongoing litigation and legal issues, and the impact of COVID-19 on the election system and process.

Through continued support by the Democracy Fund, NGA is launching the **Governors' Election Cybersecurity Action Network** (GECAN). Through the GECAN, NGA will provide regular technical assistance through a series of webinars and state calls, written products, and state-specific support. Additionally, please reach out to NGA for any technical assistance requests, including research deep dives and connections to state and national experts. NGA can also serve as a neutral third party facilitator for conversations between state offices and bodies.

Please reach out to John Guerriero here with any questions or technical assistance requests.

GECAN Call on State Cyber Navigator Programs

The first GECAN call will take place on **Monday, July 27 from 3:00– 4:00 pm Eastern** and will examine state cyber navigator programs dedicated to election cybersecurity. We will be joined by Adam Ford, Illinois state CISO and Bill Ekblad, Minnesota Cyber Navigator, to hear about the work their programs have done to support local election officials.

Please register for the call here and reach out to John Guerriero here for more information.

NGA Webinar: Better Identity in America

Please join us for our next webinar on **Thursday, July 30 from 3:00– 4:00 pm Eastern** to hear from Jeremy Grant, who leads the Better Identity Coalition and Oklahoma's Secretary of Digital Transformation and Administration, David Ostrowe. Our guests will discuss the Better Identity in

America: A Blueprint for Policymakers, which outlines policy recommendations for improving the privacy and security of digital identity solutions, focused on promoting the development and adoption of better solutions for identity verification and authentication. The blueprint is particularly relevant during the COVID-19 pandemic, as many in-person public and private sector services have been shuttered and inadequacies in the nation's digital identity infrastructure have posed major challenges in offering secure online alternatives. State governments are critical to the digital identity environment as they are one of the few authoritative issuers of identity and the proposed new revisions to the REAL ID Act would enhance that role.

Please register here for the webinar and reach out to Khristal Thomas here for additional information.

Recent NGA Memos:

Cybersecurity Concerns for Health and Public Health Institutions
As health organizations rapidly address and adapt to the challenges presented by COVID-19, cybersecurity resilience should be prioritized.. NGA released a memo outlining prevailing vulnerabilities within health information technology, current threat landscapes and cybersecurity best practices for health and public health organizations.

Countering Mis- and Disinformation Amid COVID-19
Mis- and disinformation campaigns have exploited the COVID-19 pandemic to undermine the credibility of public health guidance, influence public opinion, and deepen societal divides. NGA released a memo examining the current landscape and available resources, while recommending actions states can take to counter these campaigns.

NGA Request for Information:

1. What creative public-private partnerships has your state leveraged to add to its existing federal and state funding sources for cybersecurity?

2. How has your state worked to reduce overall risk to local governments? Have there been certain authorities, incentives, and/or regulations that have had a significant impact?

3. Has your state conducted concrete steps to improve local governments' cyber preparedness programs? If so, what services are provided?

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

Cybersecurity Resources

CISA Resources

Cyber Essentials Toolkit Chapter 2 Released

DHS' Cybersecurity and Infrastructure Agency (CISA) released the second in a series of six toolkits supporting its 2019 Cyber Essentials guide. Chapter 2 emphasizes the importance of an organizational culture of cyber readiness and greater cyber awareness among staff. Read more about CISA's Cyber Essentials here and access Toolkit 2 here.

Mis- and Disinformation Toolkit

CISA released a toolkit for state, local, tribal and territorial officials to help spread awareness of the mis- and dis information campaigns surrounding COVID-19. The toolkit includes talking points, FAQs, and outreach posters. Access the toolkit here.

Critical Vulnerability Alerts

CISA recently released several alerts on major system vulnerabilities, including:

- Windows DNS Server
- SAP Netweaver AS Java
- Treck TCP/IP Stack (Ripple 20)
- BIG-IP Traffic Management User Interface (CVE-2020-5902)

Massachusetts Cyber Center Cyber Toolkit for Municipalities

The Massachusetts Cyber Center developed and released a toolkit to help municipal leaders understand their cybersecurity posture and basic steps towards protecting municipal infrastructure from cyber threats. The toolkit includes guidance for initiating conversations on cybersecurity and cyber threats, business planning, and centralizes resources from national experts on cyber hygiene, ransomware, and risk management.

Cybersecurity Lessons from the Pandemic

The Cyberspace Solarium Commission released its first white paper examining observations from the COVID-19 pandemic as they relate to cybersecurity and cyber disruption response. The paper highlights many of the recommendations the Commission made in its March report, but introduces four new recommendations on IoT legislation, establishing a Social Media Data and Threat Analysis Center, assistance for non-profits working on countering cybercrime and supporting victims, and building non-governmental capacity to identify and counter disinformation campaigns. Read the white paper here.

Cybersecurity Information Sharing Success Stories

Researchers at the University of Albany released a paper highlighting success stories in information sharing across several different sectors. The

paper offers insight both to and from a range of sources, including policymakers, information sharing organizations and organizations deciding whether to enter into formal information sharing structures. Access the paper here and read more about the study from this Lawfare post.

Digital Contact Tracing Tools for COVID-19 Mitigation

The Belfer Center at Harvard's Kennedy School released its report, Considerations for Digital Contact Tracing Tools for COVID-19 Mitigation: Recommendations for Stakeholders and Policymakers. The report highlights Google and Apple's Bluetooth proximity method as well as the use of location services in contact tracing software applications. The report offers extensive recommendations for state and local governments and calls for a National Coordinating and Convening Body to provide states a clearinghouse for best practices and expertise on scaling digital tracing. Read more about the report here.

Perceptions of Partisan Political Bots

A recent study examines how perceptions of Twitter bots relate to users' partisanship. Findings include that users find identifying bots difficult and that perception of whether certain accounts are bots or human tend to fall along partisan lines. Read more about the study here.

K-12 Cybersecurity Education Survey

A national survey of K-12 educators from CYBER.ORG and administered by the EdWeek Research Center found that cybersecurity education is often not offered in many schools, and more likely to be provided in affluent districts when it is. See the survey here.

Election Security Resources

CISA Election Cybersecurity Guides

CISA released its Innovative Practices and New Solutions Guide, which provides guidance to election officials on how to administer and secure election infrastructure in light of the COVID-19 pandemic. Read the guide here.

CISA also published its Cyber Incident Detection and Notification Planning Guide for Election Security to help support election officials in identifying and responding to potential cyber incidents. The guide also includes templates for incident response and recognition. Read more about the guide here.

Brennan Center Report on Preparing for Cyberattacks

Election security experts at the Brennan Center for Justice at NYU Law School have released a report to help election officials prepare for cyberattacks and technical problems that may arise due to the rapid shifts in election administration caused by COVID-19. The report provides

guidance on protecting voter registration systems, mail-in voting, in-person voting, results reporting and public communications. Access the report here and the checklist here.

Cybersecurity News

Congressional Leaders Request Counterintelligence Briefing from FBI

Democratic Congressional leaders sent a letter to the FBI Director requesting a defensive counterintelligence briefing to all members of Congress on foreign efforts to intervene in the 2020 election. The letter warns that foreign interference campaigns may seek to launder and amplify disinformation through members of Congress. Read the text of the letter here.

State and Local Government Role in Public Cyber Safety

NGA's Maggie Brunner authored an op-ed emphasizing the role state and local government leaders have in protecting citizens from cyberspace threats, especially as remote work becomes normalized and cybercrimes targeting individuals continues to rise. Read more here.

States Pilot a Cybersecurity Automation Program

Johns Hopkins University is working with the IT agencies in four states (AZ, LA, MA and TX) and Arizona's Maricopa County to pilot a program that automatically acts on cyberthreat intelligence instead of relying on manual entry. The agencies will be using the Security Orchestration, Automation and Response (SOAR) tools. The pilot program, which is supported by CIS and CISA, will attempt to reduce the response time to indicators shared by the MS-ISAC. Read more here.

New York Investigating Twitter Hack

New York Governor Andrew Cuomo announced that the state's Department of Financial Services will conduct its own investigation of the recent cyberattack against Twitter. In addition to politicians and celebrities, the attack targeted accounts belonging to cryptocurrency exchanges, which are regulated by the state. Read more about the New York investigation here.

After an investigation, Twitter revealed that an internal employee tool was used to exploit the hacked accounts and a social engineering campaign was used to target its employees. Read more about the Twitter cyberattack here.

Russia Targeting COVID Vaccine Data

U.S., British and Canadian intelligence officials have linked ATP29, a threat group associated with a Russian intelligence agency, to attempts to

steal intelligence on vaccines from universities, companies and health care organizations. The U.S. government has also previously warned about Chinese and Iranian efforts to steal vaccine research. Read more about the alleged Russian attempts here. CISA and the NSA released a Joint Cybersecurity Advisory with agencies from the UK and Canada to expose the threat. Read the joint advisory here.

Election Security News

EAC Panel on Lessons Learned from 2020 Primaries

The U.S. Election Assistance Commission (EAC) held a hearing with state and local election officials on how lessons learned from their primary elections may apply to the general election in November. The officials discussed the urgency for recruiting and training younger poll workers, expectations for widescale vote-by-mail, and the need for additional funding for PPE and safety measures. Read more about the panel here.

EAC Offers Free Cybersecurity Training for Election Officials

The EAC also announced the immediate availability of free cybersecurity training modules for state and local election officials. The three modules are designed specifically for election administrators and look to provide foundational knowledge on cyber terminology, best practices, practical application and communication. Read more here.

Colorado Seeks to Strengthen Election Cybersecurity

Colorado Secretary of State Jena Griswold announced the formation of a five-person Rapid Response Election Security Cyber Unit to guard the state's election system from cyberattacks and disinformation campaigns. Read more here.

In June, Colorado Governor Jared Polis signed an executive order in June activating the Colorado National Guard to assist with election cybersecurity defense efforts during the state's primary. Read the order here.

Pilot Project Looks to Test the Security of Election Technology

CIS is working with federal state, and industry partners to pilot the RABET-V process to verify the security of non-voting election technology, such as electronic poll books and results reporting services. Read more about the RABET-V pilot here, and the CIS white paper on the program here.

Cybersecurity Workforce Development News

Oklahoma Offers Cybersecurity Training for Dislocated Workers

A program piloted by the Oklahoma Office of Workforce Development and CompTIA will provide 100 dislocated workers free online training, professional certification opportunities and assistance with job placement

for new technology careers. The program is supported by COVID-19 related dislocated worker funds from the U.S. Department of Labor (DOL). Read more about the program here.

Department of Labor Announces Two Funding Opportunities for Cybersecurity Training

As part of its Women in Apprenticeship and Nontraditional Occupations (WANTO) grant program, the DOL announced $4.1M in grants to community organizations to recruit, mentor, train and retain more women in quality apprenticeships programs in a variety of fields, including cybersecurity. Applicants can apply for a grant between $350k-750K for a performance period of 24 months. More information can be found here.

The DOL also announced the availability of $40 million for Strengthening Community Colleges Training Grants to support community colleges' ability to meet labor market demand for a variety of fields, including cybersecurity. Read more about the grant opportunity here.

Cybersecurity Talent Gap Remains a Critical Issue

Cyberseek, a joint initiative between the National Initiative for Cybersecurity Education (NICE), Burning Glass Technologies and CompTIA, recently released cybersecurity workforce data for the period from June 2019 through May 2020. The data shows that the ratio of cybersecurity workers to cybersecurity job openings is almost twice as low as the national ratio for all jobs and includes state-specific data breakdowns. Read more about the data here.

NGA Government Relations Updates

House Passes National Defense Authorization Act

The House passed its version of the annual National Defense Authorization Act, H.R. 6395. Read NGA's memo here summarizing key amendments offered and adopted by the House Armed Services Committee. You can access more information on cyber-related amendments in the bill here.

The Senate passed its version of the NDAA, S. 4049, this week as well. Included in the bill is a proposed amendment that would fund a cybersecurity coordinator for each state that would be responsible for working with all levels of government to prevent and respond to cyberattacks against local government, schools, research groups, and health organizations. Read more about S. 4049 here. Attached are memos from NGA's Office of Government Relations on the passage of the NDAA in the House as the Senate Armed Services Committee.

FY 2021 DHS Appropriations

The House Appropriations Committee approved the FY 2021 Homeland Security bill, which provides $50.72 billion in discretionary funding. The bill includes $2.25 billion for CISA. Details on CISA's allocation include:

- $32.6 million for cyber defense education and training;
- $6 million for Hunt and Incident Response Teams;
- $11.6 million to establish a Joint Cyber Center for National Cyber Defense;
- $19.4 million for the MS-ISAC;
- $8.1 million for cyber technical assistance to state, local, tribal, and territorial governments; and
- $25.1 million for Next Generation Networks Priority Services.

FEMA also received $700 million for the HSGP program, an increase of $140 million above FY20. Read more about the appropriations here.

H.R. 7331 – National Cyber Director Act

Representative Jim Langevin (D-RI) introduced H.R. 7331, which would establish a National Cyber Director position within the White House to serve as the president's key cybersecurity advisor. The creation of this position was among the Cyberspace Solarium Commission's recommendations. Read more about the bill here.

S. 3928 – Continuity of the Economy Act of 2020

Sen. Gary Peters (D-MI) introduced S.3928, which would direct the President to develop a continuity of operations plan for certain functions essential to the economy in the event of a cyber attack. Read more here

S.3929 – The National Guard Cyber Interoperability Act of 2020

Sen. Gary Peters (D-MI) introduced S. 3929, which would create a pilot program to allow National Guard units to provide remote cybersecurity support and technical assistance to state incident response efforts outside their home states. Read more about the bill here.

S.4195 – PROTECT Act of 2020

Sen. Jacky Rosen (D-NV) introduced S.4195, which would authorize and strengthen DHS' Cybersecurity Education and Training Assistance Program (CETAP). The bill would work to increase the education and career opportunities provided through CETAP and further develop the talent pool for cybersecurity positions. Read more about the bill here.

NGA Resource Center for State Cybersecurity Partners

- Amazon Web Services
- American Electric Power
- AT&T
- CompTIA
- Deloitte
- Proofpoint
- Rapid7
- Splunk
- Tenable
- VMware