NGA Cybersecurity Newsletter

April 7, 2020
Contact: John Guerriero (jguerriero@nga.org)
202-624-5372

Resource Center Announcements

Note: As the COVID-19 public health emergency continues, please do not hesitate to reach out to us with any questions, technical assistance requests, or ways NGA can assist. Our priority remains, as always, on being as responsive and helpful to states as possible, especially during the present crisis.

NGA Request for COVID-19 Cybersecurity Information

There has been a rise in COVID-related cyberattacks targeting state and local governments and critical infrastructure – including healthcare facilities. Understanding confidentiality issues, what types of attacks has your state broadly seen tied to COVID-19 and against which types of targets?

Additionally, how is your state responding to the cybersecurity threats posed by the COVID-19 public health emergency? Has your state issued any public guidance or advisories on the enhanced risk of COVID-19-related cyberattack? What guidance is your state providing to state and local government as they shift to remote work? Please reach out to John Guerriero here.

NGA Resources on COVID-19

NGA launched the Coronavirus: What You Need To Know website to keep Governors and states informed of the current state of the coronavirus in states and abroad, steps states and the federal government are taking to address the coronavirus, and many other resources, including a memo on the CARES supplemental aid package and a chart tracking state actions.

NGA Briefing on Cybersecurity and Critical Infrastructure

On March 20, NGA held a call with states on the impact COVID-19 on the cyber and physical security of critical infrastructure as well as any sector-specific challenges as national critical functions work to ensure continuity of operations. CISA Director Christopher Krebs and Mark Planning, Deputy Assistant Secretary of Intergovernmental and External Affairs, and Nicholas Anderson, Deputy Assistant Secretary, Infrastructure Security and Energy Restoration, joined from the Department of Energy to offer briefings to states on federal response actions. Please see NGA's notes from the call here.

Seven States Selected for NGA Workshops to Advance State Cybersecurity

Thank you to all the states who submitted applications to participate in NGA's workshop series. After a very competitive application process, NGA selected **Colorado, Michigan, Mississippi, New York, Oregon, Pennsylvania, and Tennessee** to develop action plans to improve their respective cybersecurity priorities.

RESCHEDULED: National Summit for State Cybersecurity

Thank you for your interest in attending NGA's National Summit on State Cybersecurity, originally scheduled for May 27- 29 in Rogers, Arkansas. We are committed to protecting the health and safety of our participants and have thus **decided to reschedule the Summit for a future date** due to ongoing concerns related to COVID-19. NGA will follow-up with timing and details.

NGA Request for Information

1. How is your state National Guard supporting COVID-19 response efforts? Are they supporting in a cyber capacity? Please reach out to John Guerriero here.

2. If your state has rescheduled its primary election or looking to expand vote-by-mail or absentee voting, how is your state guarding against mis and disinformation campaigns and cyber incidents? Please reach out to John Guerriero here.

COVID-19 Cybersecurity Resources

Planning and Response Guidance for State CIOs

NASCIO released a guide offering recommendations for state CIOs during the current COVID-19 pandemic, including several on preparedness and response planning, communication, supporting technology infrastructure

and services, and on increased cybersecurity risks. Read the full guidance here.

CISA Advisories on COVID-19

CISA launched a resource page specific to the outbreak containing advisories, alerts, and guidance on critical infrastructure protection and cybersecurity, particularly on COVID-19-related cyber activity, essential critical infrastructure workforce designations, teleworking, and risk management. Access the page here.

Telework Security Guidance

As the number of personnel teleworking rises across the country, so too has organizations' cyber vulnerability, as personal devices and home connections are now prime entrance points for criminal activity. Relevant news and guidance on telework includes the following:

- The FBI released guidance on defending against video-teleconferencing (VTC) hijacking – also known as "Zoombombing" when the attacks are made on the Zoom platform. The guidance recommends ensuring meetings are private – either by using a password or controlling guest access. Read the FBI guidance here.
    - Cyber criminals are also designing fake websites tied to Zoom in order to target employees. Read more here.
- The Center for Internet Security (CIS) offers a list of five network security recommendations here.
- CISA released an alert for increased VPN security here.
- Several checklists for telework area available, including from the World Economic Forum (link here) and the American Hospital Association (link here).
- Deloitte released guidance for organizations to sustain cyber hygiene during the current crisis (attached).

Spike in COVID-related Criminal Activity

The COVID-19 pandemic provides an opportunity for threat actors to target U.S. critical infrastructure, including the healthcare sector, as well as state networks and private individuals and organizations. The U.S. Health and Human Services website was recently targeted by a DDOS attack and a separate misinformation campaign spread claims via text message about an imminent nationwide quarantine.

Proofpoint has been tracking cybersecurity threats related to the pandemic. Read more about their findings here. Read more about rising national trends in criminal activity here and here.

The Federal Trade Commission released data showing a significant jump in consumer complaints related to coronavirus from consumers. The number of reports doubled in the last two weeks, totaling 7,800 since the

beginning of the year. Most of the complaints deal with online shopping, mobile texting scams, and government and business imposter scams. Read more here.

Cyber criminals are also taking advantage of the rise in online shopping. There have been several recent high-profile cases of digital skimmers swiping payment information from retail sites. Read more here.

COVID-19 State Cyber Responses

- **New York** is calling for skilled tech professionals from the private sector, research labs, and academia to assist with the state's response to the public health emergency, forming a volunteer COVID Tech SWAT team. Read more about the request here. The state also released an advisory on COVID-19-related malicious cyber activity and a guidance for telework. Read more here.
- **Virginia** and **West Virginia** both launched task forces dedicated to combatting the rising fraud schemes and cybercrime around the public health emergency. The task forces are joint federal-state initiatives in conjunction with the FBI, the states' assistant U.S. attorneys, and representatives from the state's law enforcement and Attorney General's offices.
    - Read more about Virginia's Coronavirus Task Force here and West Virginia's Coronavirus Fraud Task Force here.
- The **Colorado** Office of Information Technology added information on COVID-19 to the state government's mobile app, myColorado. The information will help provide citizens with access to government services during the state's stay-at-home order. Read more about the app here.
- The **Iowa** Department of Public Safety and **Texas** Department of Information Services released cyber advisories. Read the Iowa advisory here and the Texas advisory here.

COVID-Related Election Security Resources

- **NGA** is tracking states' primary election schedules on its coronavirus resource website. As of distribution, 12 states (CT, DE, GA, IN, KY, LA, MD, NY, OH, PA, RI & WV) and one territory (Puerto Rico) have rescheduled their primary elections due to the public health emergency.
    - Three states (AK, HI & WY) have rescheduled and canceled in-person voting for their party-run primaries.
    - Five states have taken steps to expand or ease restrictions on absentee voting for elections before November (AL, DE, IN, VA & WV). Virginia's measures also apply towards the November election.

- **NASS** released a briefing page on preparing and responding to election emergencies, including guidance and research on contingency plans and legal authorities surrounding rescheduling elections. Access their page here.
- **NCSL** launched a resource page listing available policy options and actions states have taken on their upcoming elections. Read more here. NCSL also has a site dedicated to state laws on election emergencies. Access that page here.
- The **U.S. Election Assistance Commission** (EAC) lists several resources for contingency planning, voting machine sanitation, several state-specific resources and a roundup of federal resources. Access the page here.
- **The CDC** released a guidance for cleaning and disinfecting polling places and associated voting equipment as well as ways poll workers can reduce their exposure to the virus. Read the guidance here.

Cybersecurity News

U.S. Cyberspace Solarium Commission Final Report Published

The report proposes a new cyber strategy centered on layered cyber deterrence and outlines ways the U.S. can achieve it: promoting responsible behavior in cyberspace, denying benefits to adversaries exploiting cyberspace, and imposing costs on those who target U.S. citizens, institutions, and infrastructure. The report offers legislative proposals and over 80 recommendations for both the public and private sector, including:

- Restructuring Congress to have permanent committees on cybersecurity in the House and Senate;
- Naming a Senate-confirmed Cyber "czar";
- Consolidating federal government response under CISA;
- Recommending a national data security/privacy law; and
- Creating of a Bureau of Cyber Statistics

The report also provides recommendations regarding governance, critical infrastructure resilience, workforce development and election security. Read the full report here.

CMMC Announces Varying Certification Levels for Contracts

The Department of Defense announced that its Cybersecurity Maturity Model Certification (CMMC) process will not require that all contractors meet the same certification requirement level. The announcement allows smaller subcontractors to not have to obtain the more expensive, higher level CMMC certifications that prime contractors may be required to meet. Read more about the announcement here.

Recommendations for State and Local Governments on Ransomware

A recent Deloitte report examines the trend of increased ransomware attacks against state and local governments and explores why attacks have increased, the role of cyber insurance and prevention and mitigation strategies. Read the report here.

Cyber Workforce Development News

Colorado Cybersecurity Apprenticeship Program Created Through DOL Grant

The U.S. Department of Labor announced the recipients of a $100 million grant program: Apprenticeship: Closing the Skills Gap. The program will support and scale apprenticeship expansion in a range of industries, including cybersecurity. One of the recipients, the University of Colorado Colorado Springs (UCCS), is using the grant to create and manage the Colorado Cybersecurity Apprenticeship Program (C-CAP).The C-CAP will offer ten industry certifications across five cybersecurity apprenticeship programs to train workers for mid- and advanced- level cyber roles. With partnerships across the country, the C-CAP looks to serve communities in nine states outside Colorado. Read more about the C-CAP program here and the DOL announcement here.

NIST Outlines Regional Partnerships as a Workforce Best Practice

NIST released a report highlighting regional partnerships as a critical component to addressing local workforce needs. The report highlights the accomplishments of five pilot programs NIST selected in 2016 to work towards building regional alliances. The five programs worked over the past few years to assess local workforce needs, connect workforce supply and demand, improve coordination among existing programs and retain local talent. Read NIST's full report here.

NGA Cybersecurity External Publications

Cybersecurity Program Director Maggie Brunner authored an article for the Journal of National Security Law & Policy analyzing the ways state and local governments can improve their cybercrime enforcement. Read the full article here.

In the Georgetown Policy Review, Policy Analyst Khristal Thomas examines whether internet censorship is pushing the dark web towards going commercial. Read the full article here.

NGA Government Relations Updates

Congress Passes H.R. 748 – Coronavirus Aid, Relief, and Economic Security Act (CARES Act)

The largest relief legislation ever passed by Congress, the CARES Act includes:

- $150 billion in direct aid to states, territories, tribes, and local governments for unplanned costs incurred as a result of the coronavirus crisis.
- $400 million for FEMA state grants, to include $100 million for firefighter grants, $100 million for emergency management performance grants and $200 million for emergency food and shelter program.
- $400 million to the Election Assistance Commission to distribute to states for use during the 2020 federal election cycle. The funding may be used to increase the ability to vote by mail, expand early voting and online registration, and increase the safety of voting in-person by providing more additional voting facilities and additional poll workers.
- $9 million to CISA for federal government interagency operations and support.

The full text of the bill is here. For more information on the bill, please see an NGA summary here and memo here.

NGA Resource Center for State Cybersecurity Partners

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