NGA Cybersecurity Newsletter

May 5, 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 organizations. Understanding confidentiality issues, what types of attacks has your state broadly seen tied to COVID-19 and against which types of targets? Please reach out to John Guerriero here.

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 Memo on State Cybersecurity Considerations During the COVID-19 Pandemic

NGA issued a memorandum for governors' offices outlining the COVID-themed cybersecurity threats facing states and key actions governors can take to bolster state cybersecurity. For questions about the memo, please reach out to John Guerriero here. Read the memo here.

NGA Webinar: Virtual Upskilling Opportunities in Cybersecurity – May 13 @ 1pm EDT

The NGA Resource Center for State Cybersecurity is hosting its next webinar on *Virtual Upskilling Opportunities in Cybersecurity* from **1:00 – 2:00 pm on Wednesday, May 13, 2020**. As COVID-19 continues to impact the economy, individuals – especially those unemployed, furloughed, or looking for new career opportunities – may benefit from virtual upskilling programs, including those in cybersecurity. Please join us to hear from **CompTIA** on their recent initiative offering virtual, live training courses and from **Purdue University** on the upcoming national rollout of their registered apprenticeship program in cybersecurity.

Read more about CompTIA's work in the attached one-pager and the Purdue Cybersecurity Apprenticeship Program here.

Please register for the webinar here and reach out to John Guerriero here for additional information.

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. Read NGA's release here, and a GovTech article on the program here.

NGA Request for Information:

1. Has your state developed a K-12 curriculum for cybersecurity or computer science? How did you implement and message it to stakeholders across the state?

2. What steps has your state taken to make schools and school districts more cyber secure? How was that process implemented and what tools or resources were most helpful? What measures were taken (e.g., risk assessments, remediation strategies, etc.) and what are your recommendations for other states?

3. How is your state National Guard supporting COVID-19 response efforts? Are they supporting in a cyber capacity?

4. 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 on the above requests.

Additional 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 map tracking state actions.

COVID-19 Cybersecurity Resources

COVID-19 Security Resource Library Available

The National Cybersecurity Alliance (NCSA) compiled a COVID-19 Security Resource Library to help individuals and organizations find resources to use and share. The page contains information on current scams, cyber threats and remote work. Access the library here.

Telework & Virtual Conferencing Security Guidance

- The NSA and CISA released a joint one-page guidance for public sector employees on best practices for remote work as well as what actions to avoid. The brief includes recommendations on securing the use of personal devices. Read the guidance here. CISA also released security recommendations for the Microsoft Office 365 platform. Read more here.
- CISA also has a resource page dedicated to secure telework, containing tips for video conferencing, the updated, 3.0 version of the agency's Interim Telework Guidance, as well as cyber recommendations for critical infrastructure using video conferencing. See the full resource page here.
- Tenable released a blog with recommendations for securing work from home organizations. Read the blog's recommendations here.
- Federal intelligence analysis also warns that the Zoom videoconferencing platform may be vulnerable to foreign government intrusions, including from China. Read more here.
- Proofpoint researchers have noted an increase in the use of cyberattacks using lures themed on virtual conferencing platforms. Read more about the attacks here.
- Palo Alto Networks provides an analysis of COVID-themed cyber threats and offers several incidents of compromise that can be used to increase end point security. Read the report here.

USDR Resource for State and Local Governments

As states face an unprecedented surge of traffic to digital platforms and services, cybersecurity and resilience become even more critical. U.S. Digital Response (USDR) is a pro-bono corps of technologists offering rapid staffing and expert consultation to states and local governments with critical security needs. USDR volunteers include experienced security engineers who can conduct security audits, working closely with your CISO and engineers to identify weaknesses and develop remediation

plans. You can request assistance from U.S. Digital Response on their website here or email them here.

COVID-Related Election Security Resources

- https://trustthevote.org/wp-content/uploads/2020/05/01May20_CDI-v2.pdf
- **NGA** is tracking states' primary election schedules on its coronavirus resource website. As of distribution, one state (NY) has cancelled its presidential primary, and 12 states (CT, DE, GA, IN, KY, LA, MD, NJ, OH, PA, RI & WV) and one territory (Puerto Rico) have rescheduled their primary elections due to COVID-19.
- CISA released an election security resource page to assist election officials and voters prepare for any potential effects on election security and voter registration policies and procedures. The resources were developed by the Election Infrastructure Subsector's Government Coordinating Council (GCC) and Sector Coordinating Council (SCC), and contain information on several aspects of election security, including mail-in voting and voter education. Access the 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.

Cybersecurity News

https://krebsonsecurity.com/2020/05/europes-largest-private-hospital-operator-fresenius-hit-by-ransomware/?utm_source=dlvr.it&utm_medium=twitter

Bluetooth Security a Major Issue for Exposure Notification Apps

Governments are increasingly looking to exposure notification apps using Bluetooth to track user movements to help contain the spread of COVID-19, but cybersecurity experts warn of the potential for targeted cyberattacks. Experts recommend that developers regularly test apps for vulnerabilities, implement the latest patches and updates, and that governments should ensure backend security for their databases and that the data will only be used for its intended purpose. Read more here.

Public Companies Listing Ransomware as a Top Risk Factor

Ransomware was mentioned in over a thousand SEC filings in the past year by top public companies as a credible and potential future risk for their business. Since 2018, the SEC has requested companies to improve the disclosure of cybersecurity risks and the trend reflects the cost and frequency of ransomware attacks against public corporations. Read more here.

Maryland Launches Cybersecurity Taskforce with National Guard

Responding to Maryland Governor Hogan's state emergency declaration, the National Guard, Military Department, and Department of Information Technology established a joint cybersecurity taskforce for COVID-19 response. Read more about the task force here.

WHO, Gates Foundation Emails and Passwords Posted Online

Nearly 25,000 credentials from the World Health Organization, the Gates Foundation and other organizations were posted online by an American with a history of pushing right-wing conspiracy theories. Read more here.

GAO Releases Cybersecurity Recommendations for the SBA

The US Government Accountability Office (GAO) added five priorities to their list of recommendations to the Small Business Administration (SBA), including one on improving the agency's ability to address cybersecurity threats. Read more here.

State CISOs talk Cybersecurity During COVID

State CISOs from Georgia, Utah, and Washington shared their experiences transitioning their workforces to remote work during the COVID-19 pandemic in a recent GovTech article. The CISOs discuss pre-COVID expansions of telework capabilities as well as the challenge of defending against increased cyberattacks. Read the article here.

NGA Government Relations Updates

NGA Sends Letters to Congress Urging Additional Cybersecurity and IT Investment for States

NGA, with a coalition of state and local associations, sent a letter to Congress on the need for additional cybersecurity and IT infrastructure investment due to COVID-19. Read the full letter here.

The following organizations are signatories to the letter:

- National Governors Association
- Government Finance Officers Association
- Governors Homeland Security Advisors Council
- International City/County Management Association-National Association of Counties
- National Association of Counties
- National Association of State Auditors, Comptrollers and Treasurers
- National Association of State Chief Information Officers
- National Association of State Treasurers
- National Conference of State Legislatures
- National Emergency Management Association
- National League of Cities
- The Council of State Governments

The nation's governors, through NGA, also sent a letter to Congress calling for increased COVID-19 aid, including for cybersecurity and IT infrastructure. Read the full letter here.

NGA Resource Center for State Cybersecurity Partners

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