NGA Cybersecurity Newsletter

August 7, 2019
Contact: John Guerriero (jguerriero@nga.org)
202-624-5372

Resource Center Announcements

Introducing John Guerriero – New Policy Analyst, Cyber Security, Technology & Communications

John joins the Homeland Security and Public Safety Division from NGA's Economic Opportunities Division, where he focused on workforce development, work-based learning and apprenticeships, including for cybersecurity. John earned his Master's in Public Policy from the Gerald R. Ford School of Public Policy at the University of Michigan. John originally hails from Michigan. Welcome, John!

August Resource Center Webinars:

Joint NGA & NASCIO Webinar: States Navigating Seas of Digital Identity – August 20, 2019 at 1:00pm EDT

Citizens expect a seamless transaction when doing business with state government, but there are many things that must occur to make that happen. First and foremost, how are states verifying everyone is who they say they are? Hear from Pennsylvania about how they have streamlined the citizen experience with the Keystone Login SSO initiative and how Michigan has been working on MLogin and what the next steps are for this enterprise IAM solution.

Register HERE

IoT Security: What Is It and Where Is It Heading – August 27th at 2:00pm EDT

With IoT expected to top 20+ billion connected devices by the end of the decade, a focused effort is critical if we plan to successfully secure our new IoT driven world. One of the primary necessities to meet this goal is to develop a sound understanding of what IoT is, along with methods for communication, identification, and mitigation of security issues within an IoT product's ecosystem.

During this presentation attendees will learn about the ecosystem structure of IoT and the security implication of its interconnected components, in addition to how to understand and effectively communicate the associated risk organizations will encounter as they embrace our new IoT driven world.

Register HERE

NGA Information Requests:

1. Is your state considering a training of trainers (ToT) program for its citizens around cybersecurity awareness? If so, please reach out to Maggie Brunner here.

2. Is your state providing misinformation and disinformation guidance to campaigns? If your state has advice or custom tools that it provides, please reach out to John Guerriero here.

3. 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.

CISA, MS-ISAC, NGA and NASCIO Recommend Immediate Action to Safeguard Against Ransomware Attacks

NGA, along with CISA, MS-ISAC, and NASCIO, called on state, local, territorial and tribal government partners to take action to enhance their defensive posture against ransomware. Read the full statement here.

NGA Issue Brief: State Cyber Disruption Response Plans

Published in July, the brief examines state cyber disruption response plans that governors are developing and testing in preparation for cyberattacks that demand coordination across state agencies. The plans detail the agencies that must respond to an incident, their roles and responsibilities, and how they will coordinate resources. Please find the issue brief here.

The Hybrid Benefits of the National Guard

The Law Fare post discusses the National Guard's role in modern cybersecurity policy and argues how the Guard can be a greater asset to national cybersecurity efforts. The post reviews the authorities the Guard currently has and makes recommendation for greater integration into national cybersecurity strategy and operations. Read the full post here.

NIST Releases Draft Security Feature Recommendations for IoT Devices

NIST released a “core baseline” guide, offering practical advice and outlining voluntary recommended cybersecurity features to include in network-capable devices. The guide serves as a baseline for best practices to mitigate risks associated with IoT security. Read the full guide here.

Recent Reports on Election Security

NGA staff are reading two recent reports on election security, including one from the Brooking Institute on combating disinformation studying lessons learned from Europe and a report by the Brennan Center examining six states’ funding needs for election cybersecurity.

Update from NGA’s Office of Government Relations: NGA, GHSAC, NASCIO and NCSL Coalition Letter in Support of the State Cyber Resiliency Act

NGA, GHSAC, NASCIO, and NCSL wrote Senators Gardner and Warner and Representatives Kilmer and McCaul in support of the State Cyber Resiliency Act, noting that the legislation would strengthen the nation’s cybersecurity posture through state and local cybersecurity grants administered by the DHS. Read the full letter here.

Mark Your Calendars:

September 18-20, 2019 – CISA Cyber Security Summit

State Cyber News

Louisiana Governor John Bel Edwards declared a statewide cybersecurity emergency in the wake of a number of cyber attacks against several school systems in the state. The declaration allows the state to gather resources, “including experts from the Louisiana National Guard, State Police, the Office of Technology Services, the Governor’s Office of Homeland Security and Emergency Preparedness, Louisiana State University, and others to assist the school systems."

New York Governor Andrew Cuomo signed into law the Stop Hacks and Improve Electronic Data Security Act (SHIELD Act) to "expand and update New York's data security breach notification law." The amendments will go into effect on October 23, 2019; the data security safeguard requirements will go into effect on March 23, 2020.

The US Conference of Mayors passed a resolution "calling on cities not to pay ransom to hackers who have taken over government computer systems through cyberattacks."

The NSA announced in July its intention to create a cybersecurity directorate, to become operational October 1, in an effort to "defend the US against foreign adversaries."

At least three state Attorney Generals are opening inquiries into the Capital One Breach. At issue will be interpretation of applicable states' "reasonable security" standards requirements.

NGA's Premier Cyber Champion

Raytheon

NGA Cyber Leaders

AMERICAN ELECTRIC POWER®
BOUNDLESS ENERGY™

CompTIA

Deloitte.

proofpoint.

RAPID7

tenable

NGA Cyber Pioneers

ANOMALI

AT&T

splunk>

Symantec.

vmware®

Additional Supported Provided By

NIC® the people behind eGovernment®

FireEye™

MOTOROLA SOLUTIONS