NGA Cybersecurity Newsletter

May 28, 2021
Contact: John Guerriero (jguerriero@nga.org)
202-624-5372

Resource Center Announcements

Upcoming NGA Webinar: State Cyber Governance Bodies

Please join NGA from **3:00 – 4:00pm on Monday, June 7th** for a webinar on Addressing Energy Security through State Cyber Governance Bodies. As the energy cybersecurity threat landscape continues to evolve and our dependency on digital and connected technology grows, governors are sharpening their focus on addressing cybersecurity vulnerabilities in their states. Governors often set up governance bodies such as councils, task forces, working groups or commissions to address these issues and many of those are being leveraged to improve energy security. NGA recently summarized eight states' activities in a white paper.

Registration information will be sent soon, please reach out to John Guerriero here with any questions.

Previous NGA Webinars: 5G Security Overview & Cyber EO

On May 24th, the Resource Center featured a panel of experts from AT&T for a conversation on understanding the 5G ecosystem, security risks, supply chain resilience and the challenges and opportunities that exist around deployment. You can access a webinar recording here and a PDF of the slides here.

On May 19th, the Resource Center held a briefing call on the recent cybersecurity executive order released by President Biden. The call featured Iranga Kahangama, Director of Cyber Incident Response from the National Security Council and Kelly Bissell, Global Security lead for Accenture. A PDF of the slides can be found here.

<u>NGA State Inquiries:</u>

1. Has your state drafted and implemented a statewide cybersecurity strategy? What did the process look like and does it map key cybersecurity terrain across agencies and branches of government?

2. Has your state implemented a statewide cybersecurity workforce development strategic plan? If so, what metrics are used and how do you evaluate success?

3. How has your state prepared for implementing 5G technology? Has it established any formal bodies or task forces?

Please reach out to John Guerriero here on the above requests or with any specific technical assistance requests.

Cybersecurity Resources

DHS Announces Cyber Requirements for Critical Pipeline Owners

The Transportation Security Administration (TSA) announced a Security Directive that requires critical pipeline owners and operators to report cybersecurity incidents to DHS' Cybersecurity and Infrastructure Security Agency (CISA) and to designate a Cybersecurity Coordinator, who is to be on call 24 hours a day, seven days a week. The directive also requires critical pipeline owners and operators to review their current practices, identify any gaps and remediation measures and report results to TSA and CISA within 30 days. Read the directive here.

CISA Advisory on DarkSide Ransomware

CISA and the FBI recently released a cybersecurity advisory on best practices for preventing business disruption from ransomware attacks. CISA and the FBI are urging critical infrastructure asset owners and operators to adopt a heightened state of awareness and implement the recommendations listed in this advisory. This joint advisory provides technical details on DarkSide actors and some of their known tactics and preferred targets. According to open-source reporting, DarkSide actors have been targeting multiple large, high-revenue organizations and have been observed gaining initial access through phishing, exploiting remotely accessible accounts and systems and virtual desktop infrastructure. CISA and FBI have since updated the advisory to include a downloadable STIX file of indicators of compromise to help network defenders find and mitigate activity associated with DarkSide ransomware. Read the full advisory here.

GAO Reports: Cyber Insurance & Federal Agency Supply Chain Risk

The U.S. Government Accountability Office (GAO) released a report on the current cyber insurance market, finding that take-up rates and the price of insurance has increased significantly since 2016. Likewise, the GAO also found that coverage limits have been reduced in certain sectors (e.g., healthcare and education). The report calls for increased collaboration between the public and private sector on information on cyber events and more consistent terminology and policy language. Read more here.

The GAO released a separate report on federal agencies' need to implement recommendations to manage supply chain risks. Federal agencies rely extensively on information and communication technology (ICT) products and services (e.g., computing systems, software, and networks) to carry out their operations. However, agencies face numerous ICT supply chain risks that threaten to compromise the confidentiality, integrity, or availability of an organization's systems and the information they contain. Read more here.

COVID-19 Response Spotlights Critical Role Local CIOs Play

CompTIA's Public Technology Institute published their annual study of city and county technology and workforce trends. The 2021 study focuses on ten sections, including Cybersecurity; the Impact of COVID-19 on IT Operations; The Cloud and Managed Services; Smart City/County Strategies; Emerging Tech; and State of Skills of IT Personnel. Read the full report here.

Proofpoint 2021 Voice of the CISO Report

Proofpoint released its inaugural 2021 Voice of the CISO report which explores key challenges facing chief information security officers over the past year. The report surveyed 1,400 CISOs around the world on their experience from the last year and their insights for the next 2 years. Among the findings, 66% of CISOs feel their organization is unprepared to handle a cyberattack and 58% consider human error to be their biggest cyber vulnerability. Download the report here.

CISA Potential Threat Vectors to 5G Infrastructure

CISA, in coordination with the National Security Agency, and the Office of the Director of National Intelligence, as part of the Enduring Security Framework (ESF)—a cross-sector, public-private working group—released a Potential Threat Vectors to 5G Infrastructure paper. This paper identifies and assesses risks and vulnerabilities introduced by 5G technology. Read the paper here.

FTC: Cryptocurrency Buzz Drives Record Investment Scam Losses

Since March 2020, the Federal Trade Commission (FTC) has seen a 1000% rise in the number of reported cryptocurrency scams. Nearly 7,000 people have reported losses of more than $80 million on these scams. This FTC report highlights trends in the data over the past few years and identifies different types of scams used by malicious actors. Read more here.

Cybersecurity News

Eight Virginia Universities Announce Cybersecurity Workforce Projects

Researchers from eight universities in Virginia will take part in $1 million worth of state-funded cybersecurity and autonomous vehicle-focused research projects through a statewide research initiative. The projects are designed to benefit different aspects of the cybersecurity workforce, including bio-cybersecurity and autonomous vehicle cybersecurity, as well as boosting cybersecurity startups and expanding internships programs. Read more here.

Hackers Threaten to Release Police Records, Knock 911 Offline

The Babuk cybergang that breached the Washington, D.C. Metropolitan Police Department is threatening to release the personal information of more officers if officials do not pay ransom. In April, the group breached the network and released the personal information of nearly two dozen officers, including Social Security numbers and psychological assessments. Read more here.

Public Comment Period Opens for National K-12 Cybersecurity Learning Standards

CYBER.ORG announced the opening of the public comment period for the most recent version of the K-12 cybersecurity learning standards that have been underway since September 2020. The public comment period closes on June 4th and the feedback will be incorporated into the final version of the standards, which CYBER.ORG plans to release publicly at the start of the 2021-22 school year, with voluntary adoption likely to begin in states the following year. Read more about the standards and the comment process here.

NGA Government Relations Updates

President Biden Signs Cybersecurity Executive Order

President Biden signed an Executive Order (EO) on Improving the Nation’s Cybersecurity. The EO includes several measures aimed at modernization of cybersecurity defenses and improving information sharing between the federal government and private industry. The EO ensures that IT Service Providers are able to share information with the government and requires them to share certain breach information; helps move the Federal government to secure cloud services and a zero-trust architecture, and mandates deployment of multifactor authentication and encryption with a specific time period; establishes baseline security standards for development of software sold to the government; establishes a Cybersecurity Safety Review Board, co-chaired by government and private sector leads; creates a standardized playbook and set of definitions for cyber incident response by federal departments and agencies; improves the ability to detect malicious cyber activity on federal networks and creates cybersecurity event log requirements for federal departments and agencies. Read more: Executive Order; WH Fact Sheet

President Biden Proposes Billions for Cybersecurity in American Jobs Plan

The $2 trillion American Jobs Plan includes $20 billion for state, local and tribal governments to modernize energy systems contingent upon meeting cybersecurity standards and $2 billion for grid resilience in high-risk areas. Read more here.