NGA Cybersecurity Newsletter

October 30, 2020

Contact: John Guerriero (jguerriero@nga.org)
202-624-5372

Resource Center Announcements

Recent NGA Webinars

October 26: SLTT Indicators of Compromise Automation Pilot

We recently highlighted Arizona's participation in the CISA/Johns Hopkins University Applied Physics Laboratory pilot program that looks to share information in near real-time and leverage automation to prevent and respond to cyber-attacks. We discussed the state's application of Security Orchestration, Automation and Response (SOAR) and their experiences with the pilot program, pain points and lessons learned.

During the webinar, automated workflows were referenced and shared, you can access those here. You can access the slides here and a recording here.

NGA Memo on Cybersecurity Concerns for Health and Public Health Organizations

Given the recent uptick in ransomware attacks against health infrastructure, NGA is re-releasing a memo on cybersecurity best practices for health and public health organizations, publishing with funding from the Centers for Disease Control and Prevention. Read the memo here.

NGA Memo on Health and Safety Protocols for Elections

NGA recently released a memo offering an overview of practices implemented by election officials and considerations for Governors to help reduce the risks of spreading COVID19 for the upcoming election. Read the memo here.

Managing Cyber Threats Through Effective Governance

The Center for Internet Security (CIS), the Center for Technology in Government at the University at Albany, State University of New York (CTG UAlbany), the National Conference of State Legislatures (NCSL) and NGA collaborated to create a call for action for Governors and state legislatures to create or strengthen cybersecurity governance. Read the report here.

NGA Request for Information:

1. How is your state leveraging the National Guard in preparation for the upcoming election? Will it be deployed to provide cybersecurity support? If deployed in a non-cyber capacity, what roles will it fill?

2. How is your state looking to expand and diversify its public sector cybersecurity workforce? Has your state looked at implementing public sector cybersecurity apprenticeship programs?

3. How has your state involved local jurisdictions in incident response planning? What does outreach look like? How has your state received information on local response plans and capabilities?

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

Cybersecurity Resources

NASCIO/Deloitte Cybersecurity Survey Released

The National Association of State Chief Information Officers (NASCIO) and Deloitte released their annual survey of state and territory CISOs, focusing on COVID-19, cybersecurity governance, and state and local collaboration, among other issues. Read the report here.

CISA & MS-ISAC Release Ransomware Guide

CISA and the MS-ISAC released a joint Ransomware Guide that details practices that organizations should continuously engage in to help manage the risk posed by ransomware and other cyber threats. The guide provides actionable best practices for ransomware prevention as well as a ransomware response checklist that can serve as an addendum to organization cyber incident response plans. Read the guide here.

Election Security Resources

CISA Election Disinformation Toolkit

CISA released a toolkit containing talking points and FAQs designed for election officials to emphasize their role as “trusted voices” for election information. Access the toolkit here.

CISA Releases a General Guide on Physical Security of Voting Locations and Election Facilities

CISA released a general guide on Physical Security of Voting Locations and Election Facilities. Intended for election officials, the guide encourages coordination with CISA Protective Security Advisors (PSAs) to make informed decisions about actionable steps they can take to improve their physical security posture. Read the guide here.

App Helps Election Officials In 11 States Spot Incorrect Election Information

Election officials in 11 states (AZ, CA, CO, CT, FL, GA, MD, ND, VA, WA, and WV) are using the MITRE SQUINT™ app to spot posts on social media that may contain incorrect and misleading information about elections that could discourage registered voters from showing up at the polls. The app offers a reliable way for election officials to report or correct inaccurate information and can be used to strengthen a take-down request to officials at social media channels. Read more about the app and how states are using it here.

NGA Supports #TrustedInfo2020

NGA joins the National Association of Secretaries of State (NASS) in supporting #TrustedInfo2020. The bipartisan education effort is aimed at promoting state and local election officials as the trusted sources of election information. NGA joins a host of other organizations in supporting NASS in this effort.

Registration Opens for CyberStart America

The CyberStart America program, part of the Girls Go CyberStart initiative, is available in 2020 and open to high school students of any gender. Interested states should contact Alan Paller from the SANS Institute here for more information. NGA can provide governors' offices with additional information on this program – gubernatorial announcements of the program have historically had a significant impact on student participation.

National Cybersecurity Career Awareness Week Approaching

November 9-14, 2020 marks National Cybersecurity Career Awareness Week, which looks to educate and engage students of all ages, educators, parents, and employers on the value of careers in cybersecurity. Learn more about National Cybersecurity Career Awareness Week here.

Cybersecurity News

Department of Treasury Issues Advisory on Potential Sanctions Risk for Ransomware Payments

The U.S. Department of Treasury's Office of Foreign Assets Control (OFAC) issued an advisory on the potential sanctions risk for facilitating ransomware payments. The advisory gives notice to financial institutions, insurance carriers and other institutions that facilitate ransomware payments to cyber actors on behalf of victims that doing so may violate OFAC regulations. Payments made to entities on OFAC's Specially Designated Nationals and Blocked Persons List (SDN List) or to persons in countries on the embargo list may expose those institutions making ransomware payments to civil penalties from OFAC. Read the OFAC advisory here.

Ransomware Threatens U.S. Healthcare System

A wave of ransomware attacks against U.S. hospitals and healthcare organizations poses a critical threat as COVID-19 cases are spiking across the country. CISA, the FBI and the Department of Health and Human Services (HHS) released a joint advisory describing the tactics, techniques, and procedures used by cybercriminals in the healthcare sector. Read the alert here.

U.S. Officials Warn of Foreign Election Influence Operations

The FBI and CISA released a joint alert on Iranian advanced persistent threat actors' efforts to influence and interfere with U.S. elections. The alert warns of fake media sites used to spread obtained U.S. voter-registration data and election-related disinformation. Read the alert here.

National Guard Deployed to Thwart Cyberattack in Louisiana

The Louisiana National Guard was recently called in to stop a series of cyberattacks against small government offices. Read more about the incident here.

Unemployment Fraud Reveals States Swap Cybersecurity for Speed

Many states have had an immense number of unemployment claims to process due to COVID-19 and the increased amount of fraud reveals that there are holes in identity security. Read more here.

New Jersey Cybersecurity Centralization Highlighted

During the NASCIO annual conference, New Jersey CISO Michael Geraghty made the case for their centralized cybersecurity operations within the homeland security office. The 2016 consolidation of operations into the NJ Cybersecurity and Communications Integration Cell has led to greater coordination between state agencies, local government and federal authorities, and greater efficiency at intercepting cyber threats. Read more here.

How State IT Officials Ramped Up Capacity, Security as Workers Went Remote

State chief information technology officials discussed the unique challenges surrounding the move to a remote environment on a panel during the NASCIO virtual conference. Read more here.

West Virginia Quickly Builds Statewide Network for Students

West Virginia established the Kid Connect Initiative, a unified education network that enables hundreds of Wi-Fi access points across the state for K-12 and college students. The project started in early August to connect students from any access point within a network spread over the state. By

September, the state had set up 850 locations and continues to install sites. Read more about the initiative here.

Cyber Workforce Development News

Old Dominion University (ODU) Launches Cybersecurity School

ODU's Center for Cybersecurity Education and Research is now the School of Cybersecurity and is the first research university in the country to open a school of cybersecurity. The program has grown from 11 students in 2015 to around 800 in 2020. The new school opened on Oct. 1 with expanded degree offerings for students seeking bachelor's and master's degrees. Read more about the school here.

Department of Defense and National Security Agency Announce New Initiative

The DOD and the NSA announced a new workforce development program that looks to redefine the academic path for cybersecurity careers. The Cybersecurity Education Diversity Initiative (CEDI) will work to improve access to certified teachers, quality education resources, mentoring opportunities and geographically located internships. Read more here.

Wright State University Program to Develop Cybersecurity Workforce

WSU has been awarded a three-year contract from the Air Force to develop the next generation of engineering students with the skills to design and develop digital microelectronic devices and systems. The program will address the current gap in academic programs across the country with expertise in assured and trusted microelectronics. Read more about the program here.

NGA Government Relations Updates

NGA Outlines NDAA Priorities

NGA sent its top priorities for the Fiscal Year 2021 National Defense Authorization Act (NDAA) to leaders of the House and Senate Armed Services committees. These asks include provisions related to National Guard cybersecurity support and more effective and transparent utilization of the National Guard during catastrophic disasters and pandemics. Read the letter here.

House Passes H.R. 5823 – State and Local Cybersecurity Improvement Act

The House passed H.R. 5823, the State and Local Cybersecurity Improvement Act, which would establish a $400 million state and local cybersecurity grant program through DHS. The bill is sponsored by Rep. Cedric Richmond (D-LA). Read more here.

Bill Introduced in Senate to Support National Guard Role in State and Local Cybersecurity

Senators Maggie Hassan (D-NH) and John Cornyn (R-TX) introduced a bill to the Senate that would amend Title 32 to include critical infrastructure cybersecurity operations as part of training and other duties of federally activated National Guard service members. Read the bill text here.

NGA Resource Center for State Cybersecurity Partners

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