NGA Cybersecurity Newsletter

February 26, 2020
Contact: John Guerriero (jguerriero@nga.org)
202-624-5372

Resource Center Announcements

National Summit for State Cybersecurity: May 27-29 in Rogers, Arkansas

NGA invites you to the **Fourth National Summit on State Cybersecurity from May 27 – 29, 2020 in Rogers, Arkansas.** As the only national meeting focused on state cybersecurity, this unique event will convene governors' offices, state homeland security advisors, chief information officers, chief information security officers, National Guard leaders and others from all 55 states and territories. Participants will engage in a series of interactive sessions sharing innovative solutions to address the evolving threat landscape. More information, including hotel and registration details, is forthcoming.

Request for Speakers
We are opening a Call for Speakers to allow states and territories to submit proposals for presentations related to any aspect of state cybersecurity. The deadline for submission is **March 9, 2020**. Click here for more details.

Please direct any questions to John Guerriero here.

NGA Request for Applications: Workshops to Advance State Cybersecurity

NGA is pleased to offer states a technical assistance opportunity: NGA Workshops to Advance State Cybersecurity. Selected states will receive hands-on technical assistance from the NGA Resource Center for State Cybersecurity, including an in-state workshop. NGA will partner with selected governors' offices to build capacity to address a wide range of objectives in state cybersecurity, including those listed below.

NGA will select up to six (6) states presenting projects around the following strategic priority areas:

I. Cybersecurity Governance;
II. Cybersecurity Workforce Development;
III. Critical Infrastructure Security;
IV. State-Local Partnerships on Cybersecurity; or
V. Innovations in State Cybersecurity

Please see the Request for Applications (RFA) here and for more information, reach out to Maggie Brunner here. Applications are due **March 3, 2020 at 8pm ET/5pm PT**.

Governors Call on Congress to Authorize Cybersecurity Grant Funding

NGA released a statement urging Congress to pass legislation this year that would provide dedicated grant funding to states and localities to help strengthen their cybersecurity posture. With several pieces of cyber legislation before Congress this year – including S.1065/H.R. 2130, the State Cyber Resiliency Act, S.1846 the State and Local Government Cybersecurity Act of 2019 and H.R 5823 the State and Local Cybersecurity Improvement Act – there is an opportunity to lay the groundwork for increased funding and resources to help states and localities improve their preparation, response and recovery efforts related to cyber incidents. Read NGA's statement here.

Resource Center Webinars

COOP & COG Planning: March 30, 2020

Please join us on Monday, March 30th from 3:00– 4:00 pm ET for the next Resource Center webinar on Continuity of Operations (COOP) and Continuity of Government (COG) planning. COOPs and COGs serve to ensure the continuity of essential functions under any circumstance that could disrupt normal operations. All governments and agencies should have in place viable COOP and COG plans as a baseline of preparedness for the full range of potential emergencies, especially in the wake of escalating ransomware attacks. Hear from Kevin Klein, Colorado's Homeland Security Advisor, on how to update COOP/COG plans for cyber resilience and lessons learned.

Please register for the webinar here and contact Khristal Thomas here for additional information.

State Highlight: Indiana Emergency Manager Cybersecurity Toolkit for Locals

During our most recent Resource Center webinar, we highlighted the *Indiana Emergency Manager Cybersecurity Toolkit*. We heard from the Indiana team on the role of emergency management in cybersecurity planning and response, as well as their recommendations for other states looking to create similar resources. To download the toolkit and access other resources for emergency managers, click here. Slides (PDF) and a recording (MP4) of the webinar are available.

ICYMI: NGA-NASCIO Joint Publication on State and Local Partnerships

In collaboration with the National Association of State Chief Information Officers, NGA recently released "Stronger Together: State and Local Cybersecurity Collaboration." This publication outlines promising programs that states have initiated to enhance collaboration with their local government counterparts for cyber resilience. It also provides high-level recommendations for state officials looking to strengthen partnerships with local government officials on cybersecurity. Read the report here.

NGA Information Requests:

1. What projects will your state create to meet the new requirements in the FY20 Preparedness Grants (5% of funding must be used for cybersecurity with one election security investment justification (IJ))? How are you thinking about "effectiveness" for cybersecurity projects? Please reach out to Maggie Brunner here.

2. How is your state consolidating and disseminating threat intelligence to localities? Does your state's SOC and Fusion Center categorize different security threats? Please reach out to John Guerriero here.

3. How is your state funding cyber forensic capabilities? If you have a creative approach or promising practice, please reach out to Maggie Brunner here.

4. What is your state National Guard's parameters for supporting election cybersecurity? If you would like to share more about your Guard's current efforts, please feel free to reach out to Maggie Brunner here.

5. How is your state incentivizing or supporting government agencies and businesses in your jurisdiction to adopt the NICE framework? Please reach out to John Guerriero with promising practices here.

Cybersecurity Resources

FY2020 Homeland Security Grant Program Funding Opportunity for FY2020

DHS issued a Notice of Funding Opportunity (NOFO) for Homeland Security Grant Program (HSGP) funding for fiscal year 2020. $415 million is available for the State Homeland Security Program. This NOFO places an emphasis on cybersecurity, requiring at least 5% of funding at state and local levels to be used for enhancing cybersecurity preparedness with at least one investment justification (IJ) for election security purposes. The

NOFO also requires states proactively demonstrate project "effectiveness."

Applications are due to FEMA at 5pm ET on **April 15, 2020**. Access the NOFO here and CISA's guidance on cybersecurity and soft targets categories here.

NCSC Releases New National Counterintelligence Strategy

The National Counterintelligence and Security Center (NCSC) recently unveiled the new National Counterintelligence Strategy. The strategy outlines five focus areas for national defense: national critical infrastructure, supply chain security, countering the exploitation of the U.S. economy, democratic systems, and countering foreign cyber operations. Read the full report here.

2020 Census Designated as High Risk for Cybersecurity Issues

The GAO released a report this month examining the cost and progress of 2020 census operations and flagged several cybersecurity concerns for the Census Bureau to review. Among the concerns are challenges in securing systems and data, data privacy, and managing disinformation from social media. Over the past decade, the GAO has offered 112 recommendations to the Bureau, but 28 haven't been fully implemented. Access the GAO report here.

Software Alliance Issues Policy Priorities on Cybersecurity

The BSA | Software Alliance released its key cybersecurity priorities for both the public and private sectors to address in 2020. Recommendations include securing supply chains through collaboration, developing a 21st Century workforce, and building the public sector's preparedness for digital transformation. Read the report here.

Election Security Resources

CISA Shares its Strategic Plan and TTX Package

CISA released its strategic plan for election security, outlining key priorities and partners for the upcoming elections. The plan includes information on CISA's Last Mile products as well as objectives and key actions for its four lines of effort for 2020: elections infrastructure, campaigns and political infrastructure, the American electorate, and warning and response. Read the full plan here.

CISA also released a package of election cybersecurity tabletop exercises that it developed for state, local, and private sector partners. The package includes template exercise scenarios, objectives, and discussion

questions. Interested parties can request an editable Word version from CISA or access the PDF here.

Iranian Digital Influence Efforts on the Rise

The Atlantic Council released a report urging the federal government to improve its efforts to counter Iran's growing digital influence campaign. While Russian efforts receive most of the publicity, Iran's accumulating investment and experience in digital influence operations should not be overlooked, especially considering recent tensions, the report warns. Read the full report here.

Facebook also recently took action against malicious actors from Iran, Russian, and Myanmar that deployed fake accounts to manipulate users. The accounts with ties to Iran specifically targeted U.S. users on religious and geo-political issues. The accounts with ties to Russian military intelligence services primarily targeted Ukrainian users while the Myanmar accounts were tied to Myanmar and Vietnamese telecom providers looking to disparage competitors. Read more about Facebook's actions here. Twitter also recently suspended a large number of accounts with ties to Iran that suggested the involvement of the Iranian government. Read more here.

Handbook for Local Election Officials

With security concerns at the forefront of the 2020 election, the Alliance for Securing Democracy offers several recommendations for local election officials in their recent release. Recommendations include adding cyber expertise to local offices, forming local working groups on election cybersecurity, securing county websites through .gov domains, reducing vulnerability to insider threats, and working with state officials to protect the voter registration process. Read more about the recommendations here.

Researchers Identify Vulnerabilities in Mobile Voting Platform

While that has been a rise in interest nationally to use mobile technology to improve voter accessibility, cybersecurity experts against the accompanying security concerns that approach presents. The most recent study on the vulnerabilities with mobile voting technology comes from MIT and highlights the security concerns with a specific mobile voting app, Voatz, which is in use in several jurisdictions across the country. Their findings illustrate weaknesses in the app, including opportunities for hackers to alter, stop, or expose how individual users vote. Read more about the analysis here and the technical paper can be found 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. #TrustedInfo2020 aims to reduce the misinformation and disinformation surrounding elections by directing voters directly to election officials' websites and social media pages. NGA joins a host of other organizations in supporting NASS in this effort.

Cybersecurity News

Cyber Standards for DoD Contractors Finalized

The Department of Defense issued final standards under the Cybersecurity Maturity Model Certification (CMMC). The framework consists of five levels of security standards under which DoD contractors will be required to comply. Under the standards, contractors will be required to pay a CMMC-certified assessor to perform a physical assessment of their operations to ensure compliance with one of the five levels. A non-profit board comprising industry and academic stakeholders are tasked with training and overseeing the assessors. Read more about the CMMC model here.

Phishing Concerns Rise with Coronavirus

Malicious actors are using the outbreak of the coronavirus to lure people to click on links and open attachments containing malware. Several campaigns have targeted Japanese and Indonesian citizens. As concern over the virus grows, the malware campaigns will grow more persistent. Read more here.

State Officials Press Congress for More Resources to Fight Cyberattacks

The Senate Homeland Security and Governmental Affairs Committee heard from CISA Director Chris Krebs, Michigan Chief Security Officer Chris DeRusha, and Texas Department of Information Resources Director Amanda Crawford on the pressing need for more resource allocation to state and local governments to fight cyberattacks. The testimonies called on the need for designated officials assigned by CISA to each state to assist on cybersecurity issues, improved threat information sharing between federal and state government, and reduced response times for federal support to locals experiencing a cyber incident. Read more about the hearing here.

State and Federal Partnerships Key to Critical Infrastructure Protection

Former Connecticut CISO and current Communications Director at Office of the Director of National Intelligence Arthur House calls for increased coordination and collaboration between federal and state governments to address key gaps in critical infrastructure cybersecurity. House calls for the national security planning process to incorporate states more, especially given their significant roles in overseeing essential services and emergency response. Read the op-ed here.

Cyber Aspects of Trump Budget

President Trump's recently released fiscal 2021 budget request shows a proposed $158 million cut to CISA while increasing DoD's cyberspace budget from $9.6 billion to $9.8 billion. Read more about the proposed budget here, and the full request here.

IBM Apprenticeship Program Helps Bridge Cyber Workforce Gap

IBM's registered apprenticeship program in cybersecurity is highlighted in this feature. Launched in 2017, the program has trained nearly 200 apprentices on skills such as JavaScript, Python, and C#. IBM is part of an employer coalition supporting the Aspen Institute in identifying principles for growing and sustaining the nation's cybersecurity workforce.

Safer Internet Day Raises Cybersecurity Awareness Across Country

Tuesday, February 11 marked Safer Internet Day, an international campaign to raise awareness on the risks associated with increased digital device activity and internet use, including cyberbullying and cyber-attacks. States across the country participated in the initiative, using the day as an opportunity to promote cyber hygiene best practices and other helpful information. The Maryland State Police offered a list of tips for parents and senior citizens, while the Rhode Island National Guard stressed the importance of building relationships with local governments to help guard against ransomware.

Virginia Seeks to Quantify Cyber Risk More Accurately

The Virginia Information Technology Agency (VITA) is in the process of implementing a new model to offer a more accurate estimate of the cyber risk facing the state. The model draws from several existing frameworks, including the Factor Analysis of Information Risk (FAIR) and Center for Internet Security (CIS) frameworks. Read more here.

Election Security News

AZ Secretary of State Highlights the State's Effort Election Security

Arizona Secretary of State Katie Hobbs wrote an op-ed highlighting the efforts that the state has taken to ensure the security of the state's elections. Secretary Hobbs' office has worked with county election officials as well as Governor Ducey's office on several initiatives, including hosting the state's first ever table-top exercise involving top officials from each county as well as key state and federal partners. Arizona participated in NGA's Policy Academy on Election Security in 2019, focusing on incident response and communications planning. Read the op-ed here.

Highlights from NASS and NASED Winter Conferences

The National Association of Secretaries of State (NASS) and National Association of State Election Directors (NASED) recently concluded their winter meetings in Washington, D.C., convening both state and federal election security officials to discuss challenges, trends, and best practices. Materials from the sessions can be found at the following links:

- NASS materials
- NASED materials

Georgia Counties All Join the EI-ISAC

Georgia Secretary of State Brad Raffensperger announced that all of Georgia's 159 counties have joined the Elections Infrastructure ISAC. Read the release here.

Select NGA Government Relations Updates

H.R. 5760 – Grid Security Research and Development Act

The House Homeland Security Committee referred H.R. 5760 to the Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation. The bill would increase research and development initiatives to boost the capacity of the energy sector to prepare for and resist cyberattacks. Read the full text of the bill here.

H.R. 5823 — State and Local Cybersecurity Improvement Act

The House Homeland Security Committee advanced H.R. 5823, which would establish a $400 million grant program to assist state and locals in strengthening their network security. Read the full text of the bill here.

NGA Resource Center for State Cybersecurity Partners

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