NGA Cybersecurity Newsletter

April 29, 2021

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

Resource Center Announcements

NGA Paper on Cybersecurity of Critical Energy Sector

NGA's new paper reviews eight states that have made a concerted effort to address vulnerabilities facing the cybersecurity of the critical energy sector through a statewide governance body. This paper addresses practices Governors can follow to establish effective cybersecurity governance bodies that support critical infrastructure cybersecurity, with a focus on the energy sector.

NGA Policy Academy on Advancing Whole-of-State Cybersecurity Launches

As NGA's Policy Academy gets underway, this GovTech article examines the work that three of the five states are looking to accomplish over the course of the next year. Read more on Indiana's, Kansas' and Montana's projects here.

NGA Requests for Information:

1. Is your state considering any cybercrime enforcement-related legislation?

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 assessed its cybersecurity labor market? Have you inventoried industry needs or how many educational and training organizations are offering cyber certificate and degree programs?

4. Has your state adopted a registered apprenticeship program in cybersecurity or information technology for public sector entities? How did you develop the program standards and curriculum and market it to both candidates and within the state?

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

Cybersecurity Resources

Framework for Countering Ransomware Released

A ransomware task force convened by the Institute for Security and Technology and comprised of experts across industry, government, nonprofits and academia released its report, offering 48 recommendations. The framework centers around four goals: deterring ransomware attacks through a nationally and internationally coordinated and comprehensive strategy; disrupting the ransomware business model; assisting organizations prepare for attacks and responding to them more effectively. Read more about the report here.

Joint Advisory on Russian Cyber Operations

The FBI, DHS and CISA released a joint advisory that outlines the targets, tools and capabilities of Russian Foreign Intelligence Service (SVR) cyber actors. These actors, who the White House attributed the SolarWinds compromise to, primarily target government networks, think tanks and other policy analysis organizations, and information technology companies. The alert outlines the SVR's tactics, techniques and procedures and provides recommendations for organizations on defending against them. Read the advisory here. The advisory complements a prior joint cyber advisory regarding the SVR exploiting five publicly known vulnerabilities.

DoD Inspector General: Telework Increased Hack Risks

In a recent report, the Department of Defense's inspector general noted that the DoD "did not consistently maintain network protections" as the agency's workforce went remote. The report notes failures of some offices to patch known vulnerabilities in VPNs. Read the report here.

FBI Releases the IC3 2020 Internet Crime Report

The FBI's Internet Crime Complaint Center (IC3) has released its annual Internet Crime Report for 2020. The top three crimes reported by victims in 2020 were phishing scams, non-payment/non-delivery scams, and extortion. State-specific statistics have also been released and can be found within the 2020 Internet Crime Report and in the accompanying 2020 State Reports. Read more here.

Recent Reports from Partner Organization NASCIO

NASCIO, in conjunction with the Center for Internet Security (CIS) and the National Association of State Procurement Officials (NASPO), released a publication outlining how state governments can make cybersecurity central to the acquisition process. Read more here.

In March, NASCIO also released a report on a Resilient and Adaptable State IT Workforce, which details CIO workforce priorities and lessons learned from the COVID-19 pandemic. Read the report here.

DOL Announces Funding Opportunity for Women in Cyber Apprenticeships

The U.S. Department of Labor recently released a notice of funding opportunity aimed at supporting women in registered apprenticeship programs and non-traditional occupations, including cybersecurity. The grant opportunity will look to award $3.5 million for up to ten grants. Read more about the opportunity here.

Cybersecurity News

No Cost Dot Gov Domain Now Administered Through CISA

With the enactment of the DOTGOV Act, the .gov top level domain has transitioned to management under CISA and is now available to qualifying state, local tribal and territorial government entities for free. Read more about the transition here.

Indiana Bill Increases Cybersecurity Information Sharing

The Indiana legislature recently passed HB 1169, which Governor Eric Holcomb is expected to sign, expands the Indiana Office of Technology's (IOT) role in cyber incident reporting and response efforts. The legislation requires state agencies and local governments to report any cyber incidents to the IOT within two business days and enables the IOT to develop a cyber incident repository. The bill also looks to provide more authority for the IOT to work with state agencies and local governments on security. Read more here.

State Cybersecurity Team Moves to Arizona Department of Homeland Security

Arizona Governor Doug Ducey announced the appointment of state CISO Tim Roemer as Director of the state's Department of Homeland Security. As part of the change in leadership, the cybersecurity operations overseen by Roemer will become part of the Department of Homeland Security. Previously, cyber operations were housed in the Arizona Department of Administration. Read more here.

2021 Developments in State Cybersecurity Safe Harbor Laws

Utah and Connecticut recently enacted or introduced safe harbor legislation that incentivizes businesses to protect personal information by adopting industry-recognized cybersecurity frameworks such as NIST Cybersecurity Framework and the CIS Top 20 Critical Security Controls. Read more here.

DC Police Department Data Leaked

Washington, D.C. Metropolitan Police Department files and data were accessed and leaked recently by actors associated with the Babuk malware, an emerging form of ransomware. Read more here.

DOJ Creates Task Force to Combat Ransomware Cyberattacks

The U.S. Department of Justice (DOJ) formed a task force to curtail the proliferation of ransomware cyberattacks. The task force will consist of the Justice Department's criminal, national security and civil divisions, the FBI and the Executive Office of U.S. Attorneys, which supports the top 93 federal prosecutors across the country. The taskforce will look to increase collaboration with the private sector, international partners, and other federal agencies. Read more here.

DOE Launches Plan Addressing Cyber Risks to Electric System

The U.S. Department of Energy (DOE) announced a 100-day effort to enhance the cybersecurity electric utilities' industrial control systems. The DOE's Office of Cybersecurity, Energy Security, and Emergency Response (CESER) will collaborate with CISA on this initiative. Read more here.

IBM Grants to Help School Districts Better Prepare for Cyberattacks

IBM Education Security Preparedness Grants will help six U.S. public K-12 school districts better prepare for cyberattacks. The grants will be distributed via the IBM Service Corps program, which would deploy teams to proactively prepare for and respond to cyber threats. Read more here.

New Mississippi Law Requires Computer Science in Schools

Mississippi Governor Tate Reeves signed House Bill 633 last week that requires the state Department of Education to create a computer science curriculum for all elementary, middle and high schools by the 2024-25 academic year. Read more here.

NGA Government Relations Updates

Biden Administration Moves on Cybersecurity

Executive Order Sanctions Russian Foreign Activities

President Biden signed a sanctions executive order targeting Russia's foreign activity, including its efforts to undermine U.S. elections and malicious cyber activity against the US and its allies. Pursuant to the order, the U.S. Department of Treasury designated six Russian technology companies that support the Russian Intelligence Services' cyber program and also sanctioned 32 entities and individuals linked to attempting to interfere with the U.S. election. Also included in the order was the official White House attribution of the SolarWinds compromise to the Russian Foreign Intelligence Service (SVR). Read more here.

Senior Cyber Appointees Named

President Biden announced his intention to nominate a slate of senior officials charged with securing the nation's cybersecurity infrastructure. John C. Inglis, a former senior National Security Agency (NSA) official, is nominated as the first national cyber director; Jen Easterly, a former NSA intelligence officer who helped stand up U.S. Cyber Command, is nominated to head CISA, and Robert Silvers, who served as DHS' Assistant Secretary for cyber policy in the Obama administration, as undersecretary for policy at DHS. The announcement includes announcements for other DHS senior officials. Read the White House press release here.

National Emergency on Cyber Activities Continued

President Biden issued a notice that his Administration will continue the national emergency related to malicious cyber-enable activities. The notice states, " significant malicious cyber-enabled activities continue to pose an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States." The original national emergency was declared on April 1, 2015 by Executive Order 13694. Read the White House Notice here and the Letter to Congress here.

Governor Ige Testimony on DHS Preparedness Grant Programs

Alongside other state and local leaders, Hawai'i Governor David Ige testified to the House Subcommittee on Emergency Preparedness, Response, and Recovery on the role that DHS preparedness grants play in protecting citizens and communities. Representing the National Governors Association, Governor Ige's testimony included governors' priorities on cybersecurity, including addressing the role the federal government plays in supporting state and territory governments during a cyber incident, response planning, and establishing a dedicated state, territorial and local cybersecurity grant program. See Governor Ige's full testimony here.

House Approves Bill for State Department to Open a Cyber Bureau

The House passed H.R. 1251, the Cyber Diplomacy Act, which would require the State Department to create the Bureau of International Cyberspace Policy, which would look lead the Department's work with the international community on cyberspace issues. Read more here.

Cyber Response and Recovery Act Introduced

Senators Gary Peters (D-MI) and Rob Portman (R-OH) introduced S. 1316, the Cyber Response and Recovery Act, which would give the DHS Secretary, in consultation with the National Cyber Director, the authority to declare a "significant cyber incident" after a breach of public or private networks. Under the declaration, CISA would have the authority to coordinate response efforts at both the federal and non-federal levels and

also access a Cyber Response and Recovery Fund to assist affected entities. The legislation would codify a recommendation made by the Cyberspace Solarium Commission. Read more here.

National Risk Management Act Introduced

Senators Maggie Hassan (D-NH) and Ben Sasse (R-NE) introduced a bill that would direct CISA to establish a risk management cycle, where DHS would identify and report on emerging threats to critical infrastructure, including cyber, to Congress. Additionally, the White House would have to report to Congress on a national critical infrastructure resilience strategy to address those risks identified by the DHS Secretary. Read the bill here.