READY NATION:
POLICY

NEMA
NATIONAL EMERGENCY MANAGEMENT ASSOCIATION

a collaborative environment to drive policy, innovate and advance emergency management

May 14, 2021

THIS WEEK IN WASHINGTON:

Mask Off

News flew from all corners of the federal interagency this week, with a notable change in guidance from CDC regarding masking while vaccinated (or the lack thereof). This morning, leaders of the House Homeland Security Committee announced an agreement to create a bipartisan commission to review the attack on the Capitol on January 6, which will be similar in design to the 9/11 Commission. However, not all members of House leadership are on board as of yet, so adjustments may still be made to the size and scope of the investigation. More information is available here.

And as you can see from our additional news items below, it was cybersecurity week this week – although not by intentionally coordinated policy roll out, but because of the Colonial Pipeline ransomware attack and its implications. Expect cybersecurity to be a central topic of discussion on the Hill and across the federal government all year as Acting CISA Director Brandon Wales said this week that Congress should enact a law requiring critical infrastructure owners and operators to report cyber incidents to the federal government. It is understood that Senator Mark Warner (D-VA) and some other senators are working on legislation to that effect. More here.

Hearings the Week of May 17, 2021

Examining the Role of the Department of Homeland Security's Office of Intelligence & Analysis
Senate Committee on Homeland Security & Governmental Affairs
Tuesday, May 18, 10:00am ET

Rethinking Disaster Recovery and Resiliency, Part 2: Protecting Communities and Accelerating Resilience
Senate Committee on Appropriations
Wednesday, May 19, 10:00am ET

COVID-19 Part II: Evaluating the Medical Supply Chain and Pandemic Response Gaps
Senate Committee on Homeland Security & Governmental Affairs
Wednesday, May 19, 2:30pm ET

More News from the Nation's Capital...

President Biden Signs Cybersecurity Executive Order
Given the significant cybersecurity incidents in recent months, the President signed an Executive Order focused on improving federal network security, improving information sharing between the federal government and the private sector, and strengthening incident response. As part of the EO, IT Service Providers are able to share information, including requiring the sharing of certain breach information, without contractual barriers; mandates multifactor authentication and encryption; establishes baseline standards for development of software sold to the government; establishes a Cybersecurity Safety Review Board modeled after the National Transportation Safety Board; creates a standardized playbook for responding to cyber incidents; enables a government-wide endpoint detection and response system, and; creates cybersecurity event log requirements for federal agencies.

The full Executive Order is available here (it's a long one!) and the fact sheet is available here.

DHS Announces Reorganization of Domestic Terrorism and Targeted Violence Offices
DHS established a Center for Prevention Programs and Partnerships (CP3) in an effort to improve its ability to combat terrorism and targeted violence consistent with privacy and civil rights/liberties protections. CP3 will replace the Office of Targeted Violence and Terrorism Prevention and base its work in leveraging behavioral threat assessment and management tools and addressing early-risk factors that can lead to radicalization to violence.

Within the DHS Office of Intelligence & Analysis (I&A) a new domestic terrorism branch has been established to strengthen the development of sound and timely intelligence related to domestic terrorism and targeted violence.

Additional information is available here.

State and Local Cybersecurity Improvement Legislation Introduced
Members of the House Homeland Security Committee introduced legislation to support improvements in cybersecurity at the state, local, tribal, and territorial levels. Central to the legislation is establishing a $500 million DHS grant program to SLTT governments addressing cybersecurity risks and threats to information systems. Grants can be awarded to multistate efforts.

Other elements of the legislation include requiring DHS CISA to develop a strategy to improve SLTT governments' cybersecurity, requiring SLTT governments to develop comprehensive cybersecurity plans, establishing a State and Local Cybersecurity Resilience Committee so SLTTs can advise CISA on their cybersecurity needs, and requiring DHS CISA to assess the feasibility of implementing a short-term rotational program for the detail of approved SLTT employees to cyber workforce positions at CISA.

The legislation was just introduced this week so at this time its future prospects remain unclear. Read the bill text here.

CISA and FBI DarkSide Ransomware Cybersecurity Advisory
Following the ransomware shutdown of the Colonial Pipeline DHS CISA and the FBI released a cybersecurity advisory, *DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks*. As part of the advisory, CISA and the FBI recommend critical infrastructure asset owners and operators to implement the mitigation and response actions listed. DarkSide actors have also been attacking large, high-revenue organizations, primarily through phishing, exploiting remotely accessible accounts and systems and virtual desktop infrastructure. It is now believed that Colonial Pipeline paid millions to recover its stolen data and restart operations.

View the cybersecurity advisory and other resources here.

National Advisory Committees Supporting Vulnerable Populations in Disasters Accepting Applications
The Department of Health and Human Services Office of the Assistant Secretary for Preparedness and Response (HHS ASPR) announced the establishment of two committees related to supporting vulnerable populations in disaster.

The National Advisory Committee on Individuals with Disabilities and Disasters (NACIDD) will provide the HHS Secretary with advice and consultation related to the medical, public health, and accessibility needs of individuals with disabilities in preparation for, response to, and recovery from all-hazards emergencies. The committee will include at least two SLTT representatives with expertise in disaster planning, preparedness, response, and recovery for individuals with disabilities. Applications for advisory committee membership will be accepted until June 13 (30 days from the Federal Register notice). Additional information is available here.

The National Advisory Committee on Seniors and Disasters (NACSD) will provide the HHS Secretary with advice and recommendations related to meeting the unique needs of seniors with respect to preparation for, response to, and recovery from all-hazards emergencies. The committee will include at least two SLTT representatives with expertise in geriatric medical disaster planning, preparedness, response, or recovery. Applications for advisory committee membership will be accepted until June 13 (30 days from the Federal Register notice). Additional information is available here.

Other News from DC and Around the Country:

The Hill: CDC Says Vaccinated People Can Take Masks Off Indoors and Outdoors
Pew Trust: New Collaboration Aims to Help States Prepare for, Adapt to Natural Disasters
Government CIO: SolarWinds Opened the Door for Cybersecurity Culture Overhaul at DHS

nemaweb.org