November 15, 2022

The Honorable Xavier Becerra
Secretary
U.S. Department of Health and Human Services
200 Independence Avenue, N.W.
Washington, DC 20201

Dear Secretary Becerra:

On behalf of the National Association of County and City Health Officials (NACCHO), the Big Cities Health Coalition (BCHC), and the Association of State and Territorial Health Officials (ASTHO), we write to you about the importance of including public health in cybersecurity initiatives. Like many sectors of our society, health departments rely increasingly on technology and data to carry out their mission, and threats to cybersecurity present a growing and serious challenge for public health and safety.

The Biden administration has rightfully recognized the need to strengthen cybersecurity across a range of industries and sectors, including as Deputy National Security Advisor Anne Neuberger recently discussed, an effort from the Department of Health and Human Services (HHS) to work with hospitals, medical devices, and health care partners. We urge HHS to also consider how it can support local and state health departments in strengthening their cybersecurity infrastructure and preparing for possible cyber threats. Cybersecurity efforts should consider the unique needs of health departments of different jurisdictional levels and sizes (i.e., local, state, and territorial), as well as health departments in both rural and urban settings. The Biden administration has acknowledged that cyber-preparedness will require action across multiple federal agencies, and we encourage HHS to work with other federal partners, including the Cybersecurity and Infrastructure Security Agency. As part of this cross-agency collaboration, we hope HHS will impress upon its federal partners the importance of engaging with local and state partners.

Data bear out the need to build additional health department capacity in cybersecurity. In NACCHO's 2018 Preparedness Profile Assessment Report, nearly all (93 percent) local health departments expressed concern about the impacts of the cybersecurity threats to their community in the future. In addition, only 33 percent of local health departments had conducted cybersecurity preparedness planning in the past year with even fewer local health departments doing trainings, exercises, coordination with partners, and community outreach on cybersecurity. This disparity between perceived threat and action being taken to address the threat indicates more needs to be done to promote, support, and advance preparedness efforts in this area.

Threats against public health are not theoretical: in December 2021, a cyberattack forced the Maryland Department of Health to take its website offline for days, disrupting the COVID-19 pandemic response and other routine matters for weeks.[i] While servers were down, counties were unable to see county-by-county case information, complicating efforts to deal with a spike in testing and cases. The outage also created challenges for local health departments in carrying out non-COVID-19 activities, like issuing death certificates. This year, the Fremont County Department of Public Health and Environment in Colorado was closed for nearly a month following a cyberattack.[ii] Cyberattacks have the potential to compromise individual patient records, as well as whole systems that if compromised would result in a loss of access to vital services that would disproportionately impact people who rely on the public health

safety net. Ensuring that health departments are prepared for cyberattacks is critical to the mission of protecting and promoting the health and safety of communities nationwide and we urge you to include public health and health departments in the Department's cybersecurity initiatives.

Cybersecurity efforts are also intertwined with larger HHS and public health priorities. Our organizations have been engaged with federal policymakers for years, stressing the need to strengthen and modernize the public health workforce. The workforce is the backbone of our public health system, and without the right staff in place, health departments will be ill-equipped to address an array of challenges, including cybersecurity. Therefore, we hope HHS will continue to look for ways to provide health departments with sustainable resources to bolster our workforce, including cybersecurity professionals. Cybersecurity is also key to the Centers for Disease Control and Prevention's Data Modernization Initiative. The public health system at all levels – nationally and in jurisdictions – need systems that are up to date and can adapt to the changing landscape of cyberthreats.

We would appreciate the opportunity to discuss local health department needs further and would initially suggest the Department consider how it can provide cybersecurity planning guidance, training, templates, and resources specifically for a public health audience.

We look forward to working with HHS on bolstering health department cybersecurity as part of the administration's overarching efforts to strengthen our nation's cyber preparedness. Please contact Adriane Casalotti, NACCHO Chief of Government and Public Affairs, at acasalotti@naccho.org, Chrissie Juliano, BCHC Executive Director, at juliano@bigcitieshealth.org, and Carolyn Mullen, ASTHO Senior Vice President of Government Affairs and Public Relations, at cmullen@astho.org should you have any questions or wish to discuss further.

Sincerely,

Lori Tremmel Freeman, MBA
Chief Executive Officer
National Association of County and City Health Officials

Chrissie Juliano, MPP
Executive Director
Big Cities Health Coalition

Michael R. Fraser, PhD, MS, CAE, FCPP
Chief Executive Officer
Association of State and Territorial Health Officials

Cc:
Dr. Rochelle Walensky
Director
Centers for Disease Control and Prevention

Micky Tripathi, Ph.D., M.P.P.
National Coordinator for Health Information Technology
Department of Health and Human Services

Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency

[i] https://www.washingtonpost.com/dc-md-va/2022/01/08/cyberattack-still-disrupting-maryland-department-of-health/
[ii] https://www.cpr.org/2022/08/22/cyberattack-shuts-down-fremont-county-services/