Written Testimony for the Record

Senate Committee on Environment and Public Works

"Addressing Cybersecurity Vulnerabilities Facing Our Nation's Physical Infrastructure"

Wednesday, July 21, 2021

Submitted by Evan Pratt, American Public Works Association

Chairman Carper, Ranking Member Capito, and members of the Committee, I'm Evan Pratt and on behalf of the American Public Works Association (APWA), I appreciate the opportunity to provide testimony during this important **hearing on Cybersecurity Vulnerabilities Facing Our Nation's Physical Infrastructure.**

As background, I have spent my career in public infrastructure and currently serve as the Water Resources Commissioner for Washtenaw County, Michigan, with a population of approximately 370,000, and I am a member of the APWA Government Affairs Committee. Today I am testifying on behalf of APWA and our more than 30,000 members across North America. APWA is the only association to collectively serve and represent all areas of public works responsibilities with members working in both the public and private sectors, providing expertise at the local, state, and federal levels. Cybersecurity is an increasingly important part of protecting our critical infrastructure assets and our citizenry. I'm a little embarrassed to say I am here today because I and many of my peers know we are behind on cybersecurity and we need help.

Public works professionals are first responders and we embrace our responsibilities on the front line preparing for, responding to, and recovering from disasters, while protecting our critical infrastructure. Critical infrastructure includes water and sewage treatment plants, dams, reservoirs, pumps, stormwater drainage facilities, other flood control systems, and often a variety of electronic controls for these systems.

Electronic sensors and controls for water utilities are known as SCADA systems, which stands for Supervisory Control and Data Acquisition systems. In the private sector, such as industrial plants and pipelines similar systems are often called Industrial Control Systems (ICS). For the purposes of today's hearing this is where I am focusing my testimony.

Flood control systems are critical for mitigating severe wet weather. It is essential for Congress to consider strategies to safeguard our communities from potential cyberattacks on these increasingly automated and connected

systems. Congress can support our flood control and other water infrastructure through continued and flexible federal funding, financing and regulatory streamlining to help ensure public works agencies have the resources to protect against cyberattacks.

In 2016-17, I was part of a bi-partisan task force to assess the condition and funding needs of all infrastructure in Michigan. To be clear, the overall purpose of the report was to bring ROI (return on investment) of infrastructure investment into focus relative to the state economy and quality of life, and that report is still used today. I admit there was no discussion of cybersecurity at that time, nor were any recommendations included. I have learned and observed since then that cybersecurity is an issue that still has a very unclear risk assessment profile.

On the one hand, not all utilities have remote sensing and controls. On the other, the wide range of SCADA solutions for the many who do may result in weak points when deployed, especially with varied levels of agency cyber-awareness. And particularly in the common situation where agencies can only meet their SCADA needs by stitching together products from multiple vendors and/or internal app development.

I could spend hours specifically describing how far behind hundreds of agencies are, including a breach at my County. In the interest of time today, I will just say that we can find an APWA member in your district with a story closer to home. In short, many, many government agencies have historically viewed IT infrastructure as an optional buy-up versus necessary investment. Further, the SCADA marketplace is less mature on cybersecurity than say the financial or medical software markets.

About 52,000 community water systems operate in the United States, providing water to more than 286 million people year-round. Most systems are run by local governments; many are very small. Small water utilities often do not have their own IT or cybersecurity staff. They typically are part of city or county governments, but those too may not have the staff or resources to ensure that cybersecurity is strong.

Public works professionals must be prepared to not only mitigate potential damage, but they simultaneously may also be called on to respond to and repair any such damage caused physically or otherwise from a cyber breach. Recent incidents around the nation have raised red flags that we must remain vigilant in protecting these valuable assets. The nation has seen more than its fair share of cyberattacks, just within the past year. Multiple critical infrastructure sectors have been impacted by one or more cyber incidents, both malicious and accidental with

varying degrees of impact. These include the SolarWinds and Colonial Pipeline cyber incidents and other cyber intrusions attacking SCADA systems such as Oldsmar, FL and Post Rock, KS. These all hampered aspects of the nation's critical water, transportation, energy, medical, education, and food sectors.

APWA recommends the following to improve our cybersecurity:

- The federal government must share threat information and provide technical support to state and local governments to enhance cybersecurity. One way may be by establishing **Voluntary National Cybersecurity Guidelines and** include public works in crafting these recommendations.
- Standardize and utilize important tools to protect these critical assets, including Supervisory Control and Data Acquisition (SCADA) systems, possibly consistent with tools for other ICS system protections.
- Comprehensive cybersecurity training for public works professionals to prevent and mitigate cyber intrusions.
- Continue and fully fund the Federal Emergency Management Agency's ***Emergency Management Performance Grant Program (EMPG).***
- Encourage effective asset management strategies.
- Provide robust federal funding through programs including the State Revolving Funds, Water Infrastructure Finance and Innovation Act (WIFIA) loans, and Rural Utilities Service loans & grants, making cybersecurity specifically eligible for funding.
- Financing mechanisms for water infrastructure investment at the local level should be preserved and enhanced, to allow local governments to better invest in cybersecurity. Lifting the cap on Private Activity Bonds for water infrastructure and restoring advance refunding of tax-exempt municipal bonds can assist this goal.
- Congress should continue to ensure state and local control regarding public works projects as it is the local level officials who are experts on their communities and the community needs.

Thank you to the Committee for holding this important hearing and allowing me to provide testimony. APWA stands ready to work with you towards finding effective methods to support and safeguard our infrastructure and the American public. I sit before you today because this sector is scrambling to catch up and all agencies are not on top of this – I do look forward to answering any questions you may have.