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, on behalf of the American Public Works Association (APWA), I appreciate the opportunity to provide testimony during this important hearing on **Addressing Cybersecurity Vulnerabilities Facing Our Nation's Physical Infrastructure.** It is our intention that the testimony provided will serve as a resource for the Committee.

As background, I 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.

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.

Public works professionals are first responders and have been recognized as such through Homeland Security Presidential Directive (HSPD) 8 signed by President George W. Bush in 2003. This is a designation that APWA members embrace with great pride especially when we prepare for, respond to, and assist in disaster recovery. We are responsible for protecting our critical infrastructure. Critical infrastructure includes all modes of transportation, 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. SCADA systems serve as the "nerve center" for a multitude of public works facilities and functions. 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 will focus my testimony.

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 vulnerable 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.

Public works agencies across the country are also responsible for building, operating, upgrading, and maintaining our nation's water infrastructure. This can include dams, reservoirs, stormwater drainage facilities, and other flood control systems. These systems are critical for preventing severe floods, and any attack that compromises them could endanger nearby communities. As technology advances and these systems become increasingly automated and connected, it will be critical for Congress to consider various strategies that safeguard our communities from potential cyberattacks on critical infrastructure. APWA's water resiliency policy priorities outline specifically how Congress can work with public works agencies to safeguard our infrastructure and protect public health.

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.

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.

I could spend hours specifically describing how far behind hundreds of agencies are, including a breach at my county. In the interest of time, 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.

The challenges public works professionals face today have grown to include the responsibility of safeguarding the nation's critical infrastructure from cyberattacks. Public works professionals must be prepared to not only mitigate potential damage, but they simultaneously may also be called on to respond to and or repair any damage caused physically or otherwise from a cyber breach. Recent incidents around the nation have raised red flags therefore we must remain vigilant in protecting these valuable assets that keep our nation operating. Today I look forward to sharing with you APWA's recommendations to address cybersecurity protection for our physical infrastructure. APWA understands our infrastructure and cybersecurity are interconnected and function as one on many occasions. I have included copies of APWA's public policy priorities for the 117th Congress with this testimony for the Committee's reference. These priorities, drafted by our Government Affairs Committee and approved by our Board of Directors, are reviewed and updated prior to each new Congressional session.

APWA offered strong support of the Disaster Recovery Reform Act (DRRA) when it was initially offered as a stand-alone bill during the 115th Session of Congress. Becoming law on October 5, 2018, as part of the Federal Aviation Administration Reauthorization Act of 2018, Public Law No: 115-254, the federal government now has additional tools to emphasize what public works professionals have long identified as the most important aspect of dealing with disasters – mitigation efforts. Particularly efforts to safeguard our nation's critical infrastructure such as water treatment facilities and SCADA systems. A key provision of DRRA amended the Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act), modifying the Pre-disaster Hazard Mitigation Grant Program. The modification permits the use of technical and financial assistance to establish and carry out enforcement activities to implement codes, specifications, and standards that incorporate the latest hazard-resistant designs – a valuable tool for public works professionals.

Efficient and effective communication between emergency responders, public works included, is critical for preparedness, response, and recovery operations. Public works agencies depend on reliable interoperable emergency

communications systems that connect them to other responders during response and recovery operations--including law enforcement, fire, and emergency medical professionals. APWA has been an active partner with FirstNet and provide an APWA member to the Public Safety Advisory Committee (PSAC).

With respect to this hearing, APWA believes the following aspects of our policy priorities should be highlighted and considered by this Committee to enhance our nation's ability in both the public and private sectors to address disaster readiness and strengthen our cybersecurity:

- The federal government must share threat information and provide technical support to state, local and tribal governments in order to protect computer networks and other related critical infrastructure during times of disaster governments to enhance cybersecurity. One way may be by establishing Voluntary National Cybersecurity Guidelines and include public works in crafting these recommendations. APWA fully supports the use of interagency and organization task forces to coordinate implementation of Stafford Act rules and programs, as well as issues related to critical infrastructure protection. This would include maintaining the use of cross-sector task forces and study groups. APWA looks forward to continuing to be involved in federal task forces and other groups committed to preparing for, responding to, and recovering from disasters.
- Standardize and utilize important tools to protect these critical assets, including SCADA systems, possibly consistent with tools for other ICS system protections.
- Comprehensive cybersecurity training for public works professionals to prevent and mitigate cyber intrusions, including increasing training opportunities to provide first responders with the tools to harden their facilities against potential breaches and or failures caused through malicious or accidental actions
- Continue and fully fund the Federal Emergency Management Agency's (FEMA) Emergency Management Performance Grant Program (EMPG). This program assists state, local, tribal, and territorial governments by providing direction, coordination, and guidance to ensure that an emergency preparedness system exists for all hazards.
- Encourage effective asset management strategies. More coordinated, cooperative, and communicative infrastructure management strategies that utilize comprehensive planning, data, and analytical methods will ensure that municipalities can effectively work with federal and state partners to respond to cyberattacks.

- 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, Public Water System Supervision grants, and the Public Works and Economic Development program 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.
- While APWA supports efforts to encourage state and local governments increase cybersecurity of their infrastructure, Congress should continue to ensure state and local control regarding public works projects. Local officials know their communities best.
- APWA opposes unfunded mandates that would overly burden state and local governments as they construct, maintain, and operate critical infrastructure.
- APWA recommends investment in physical and cybersecurity programs to ensure secure water resources and protect public safety. Operators of flood control infrastructure utilize automation and connected technologies which can be vulnerable to cyberattacks, and federal resources should be directed at enhanced cybersecurity of this infrastructure.
- The federal government's Environmental Protection Agency (EPA) or Department of Homeland Security (DHS) may be the proper departments to lead an effort to standardize and utilize important tools to secure communications protocols to protect these critical assets, including SCADA or ICS systems.
- APWA additionally recommends that financing mechanisms for investment in water infrastructure at the local level be preserved and enhanced to ensure that local governments have the resources to invest in the cybersecurity of their flood control infrastructure. This can be accomplished by preserving the tax-exempt status of municipal bonds, lifting the cap on Private Activity Bonds for water infrastructure, and restoring advance refunding of tax-exempt municipal bonds.
- I would urge Congress to consider acting through legislation or working with federal partners on regulatory steps. The federal government should likewise include public works in consultations pertaining to any proposed telecommunication modifications that may impact right-of-way, thereby allowing an additional

expert voice for consultation at the state and local government level to help map out where communication may be located as it may need to be accessed during an emergency.

- APWA believes the Federal Emergency Management Agency (FEMA) and the Cybersecurity and Infrastructure Security Agency (CISA) are two key components within DHS. We recommend DHS evaluate implementing practices to award grants based on estimates. Implementing these estimate-based grants would allow states to disburse funds to applicants up front (where state laws allow for such payments), rather than through the later reimbursement of actual costs. Congress enabled various pilot programs as part of the Post-Katrina Management Reform Act, Public Law 109-205, however those programs have expired. APWA supports enacting many of these pilot programs as permanent additions to the Stafford Act.

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 look forward to answering any questions you may have.

Attachment: APWA's public policy priorities for the 117th Congress--*Surface Transportation Reauthorization, Water Resiliency,* and *Emergency Management.*