Senate Committee on Environment and Public Works
Hearing Entitled, *"Addressing Cybersecurity Vulnerabilities Facing Our Nation's Physical Infrastructure"*
July 21, 2021
Questions for the Record for John Sullivan

<u>Senator Kelly</u>

1. I wanted to discuss the security of water and wastewater infrastructure. As has been discussed in this hearing, the events earlier this year in San Francisco and Oldsmar, Florida underscored the real life and safety threats that cyberattacks pose to water infrastructure. In Arizona, any similar incident could be even more catastrophic – with water users all over the state cutting back on their water reserves as a result of water shortages along the Colorado River. That's why I was incredibly proud to support the Drinking Water and Wastewater Infrastructure Act earlier this year, which expands grant funding opportunities to help water and wastewater systems and also creates a new requirement for EPA to establish a Technical Cybersecurity Support Plan for water and wastewater systems. You addressed this briefly in your testimony, but can you expand upon why additional guidance from EPA for public water systems for how to prepare for cyber threats is so critical?

   RESPONSE: The nation's drinking water and wastewater systems serve cities and towns with a wide range of resources and capabilities. In fact, roughly 97% of the nation's 50,000 community water systems serve fewer than 50,000 people, meaning that they have relatively small ratepayer bases and are likely operated with minimal staff. It would be reasonable to expect that these smaller-utility workers would be primarily focused on keeping the water flowing, and may not have the resources or expertise to stay apprised of the ever-evolving cyber threat landscape facing critical infrastructure.

   However, just because a small water system may not be focused on cybersecurity does not mean that a cyber criminal will not focus on them. We know that utilities make attractive targets to hackers who wish to sow discord or undermine public institutions, so a cyber attack that interrupts or interferes with the water supply of even the smallest water utility could have national implications for the public's confidence in their drinking water, not to mention the public health risks that would impact the customers of the affected water system.

   This is why additional guidance and resources for water systems on cybersecurity is so important. For small community utilities, even having a basic understanding of the threats – and suggested steps to mitigate those threats – can make a difference. After all, the Oldsmar incident involved outdated versions of software and less than robust password protections. With greater access to resources that promote cyber best practices, such as WaterISAC's *15 Cybersecurity Fundamentals for Water and Wastewater Utilities*, more water systems would be prompted to think about taking relatively basic steps to improve their security practices.

Just as valuable as the *15 Fundamentals* are the hundreds of water sector cyber advisories WaterISAC disseminates each year, along with alerts on vulnerabilities in the equipment and software our members use. The information that WaterISAC disseminates to the sector and maintains in its secure online library comes from many sources. In addition to the material produced by WaterISAC's analysts, WaterISAC identifies, analyzes, and shares relevant information from CISA, the FBI and other intelligence community sources, not to mention expert resources from subject matter experts in the private sector, the American Water Works Association, and from ISACs in interdependent sectors. As a nonprofit, we would like to be able to expand access to this critical information to thousands of utilities across the sector.

As my testimony noted, AMWA appreciates the rationale behind provisions in the Drinking Water and Wastewater Infrastructure Act that seek to identify and offer assistance to water systems that may be least prepared to withstand a cyber attack. We do believe the language could be improved to ensure that any lists of at-risk water systems are protected from public disclosure, as that could direct hackers as to where to direct their attention. AMWA is eager to continue to work with the committee on this issue, both to promote helpful cyber guidance from EPA, and to increase water systems' access to existing, sector-based security resources like WaterISAC.

a. Once EPA completes this guidance, do you believe that the existing federal funding streams, both through the state revolving funds and through other discretionary grant programs, that water systems will have the resources needed to harden their infrastructure to cyber threats?

   RESPONSE: AMWA believes that a dedicated source of federal cybersecurity funding assistance for drinking water and wastewater systems is an idea that should be explored. While EPA does consider water security projects to be eligible for funding through the Drinking Water State Revolving Fund, that program is primarily used by water systems to help fund projects that have a direct correlation with public health improvements or that address the $472.6 billion in investments that are needed to maintain and improve the nation's drinking water infrastructure over the next twenty years, as estimated by EPA. Against these competing needs, many individual water systems may not choose to utilize these funds to support cyber improvements.

   AMWA supports the Drinking Water and Wastewater Infrastructure Act's creation of a new Midsize and Large Drinking Water System Resilience and Sustainability Program that will offer grants to help community water systems serving 10,000 or more people pay for projects to help withstand natural hazards or reduce cybersecurity vulnerabilities. This new funding

will be valuable to these water systems. However, the legislation will also reauthorize a similar Drinking Water Infrastructure Resilience and Sustainability Program that serves small (fewer than 10,000 people) or disadvantaged community water systems, but funds through that existing program cannot be used to address cyber vulnerabilities. As a result, the smallest water systems that are likely to have the least sophistication in preparing for and responding to cyber threats will have fewer cyber grant funding opportunities than larger water systems.

Additionally, America's Water Infrastructure Act of 2018 (P.L. 115-270) authorized $25 million in each of fiscal years 2020 and 2021 for an EPA Drinking Water Infrastructure Risk and Resilience Program to help water systems address identified security risks, including through "improvements to electronic, computer, financial, or other automated systems and remote systems." While these funds would certainly be able to be used by communities to address known cyber weaknesses, to date Congress has not appropriated any funding for the program, and no grants have been awarded.

In sum, AMWA would support the creation of a dedicated federal program to improve the cybersecurity of the nation's drinking water and wastewater systems, to ensure they suffer no lack of resources to harden their infrastructure to cyber threats. Additionally, because information sharing and threat awareness must be a key part of this effort, we believe funding should also be available to subsidize WaterISAC membership fees, particularly for drinking water and wastewater systems serving fewer than 100,000 people. A modest federal investment in this area, we believe, would make great strides toward improving the cyber resilience of the water sector at large.