American Water Works Association

Government Affairs Office
1300 Eye Street NW
Suite 701W
Washington, DC 20005-3314
T 202.628.8303
F 202.628.2846

# Cyber Security and Water Utilities

**Actions Requested:**

- Enact legislation such as H.R. 3696, the National Cybersecurity and Critical Infrastructure Protection Act, that would:
  - provide greater information sharing by federal agencies about cyber threats to critical sectors such as water, including imminent cyber threats to our sector, effective measures for protecting water systems from those threats, and methods of remediation from cyber attacks;
  - formally recognize and utilize Sector Coordinating Councils and Information Sharing and Analysis Centers;
  - develop through the National Institute of Standards and Technology a voluntary, sector-led set of standards and processes to reduce cyber risks for critical sectors; and
  - expand liability protections for technology providers and water systems deploying cybersecurity technologies.

**Background:** A number of bills have been introduced in the 113th Congress addressing various aspects of cyber security. Most of them have some features which the water community could support. However, H.R. 3696 in its current form appears to be the most comprehensive and reasoned approach to cybersecurity.

The water sector's greatest need in cybersecurity is information about what threats are looming, how we can protect ourselves from them, and what steps can be done to repair the damage from a cyber attack. H.R. 3696 and H.R. 624, the Cyber Intelligence Sharing and Protection Act, both would provide this type of information (The House Committee on Homeland Security has approved H.R. 3696 and the full House has approved H.R. 624). There also needs to be recognition that different sectors may face different threats. That is why utilization of already-existing Sector Coordinating Councils is important. Each sector also already has existing expertise on cybersecurity.

In February 2013, President Obama issued Executive Order 13636 - Improving Critical Infrastructure Cybersecurity. It directed the National Institute of Standards and Technology to work with stakeholders to develop a voluntary framework for reducing cyber risks.

This past February, AWWA released the AWWA Cybersecurity Guidance & Tool, a voluntary, water sector-specific approach that supports the NIST cybersecurity framework. It can be found at www.awwa.org/cybersecurty. This guidance provides water utility managers with a concise set of best practices and standards. It puts forth a transparent and repeatable process for evaluating the security of a utility's process control system. In order to provide the widest benefit, AWWA has made the guidance and tool free and available to all water and wastewater systems. The Cybersecurity Guidance & Tool are living documents, and it is expected that future revisions and enhancements will be made based on input from government experts, users, and others. All of this illustrates that cooperation and collaboration between federal officials and sector experts is both critical and effective in cybersecurity efforts.

H.R. 3696 provides a degree of needed liability protection for the producers of cybersecurity products and processes. We recommend adding liability protection for those who use those products in good faith. Such liability protection should be extended to water systems exercising best practices in cybersecurity.

###