CIPAC Water Sector Cyber Sector Cybersecurity Strategy Workgroup Briefing

**OBJECTIVE 1:** Recommend approaches to outreach and training, including leveraging existing programs, that will promote use of the Cybersecurity Framework by all segments of the Water Sector.

**OBJECTIVE 2:** Assess gaps, if any, in available guidance, tools, and resources for application of the Cybersecurity Framework that, if addressed, would facilitate use of the Cybersecurity Framework.

**OBJECTIVE 3:** Identify measures of success that can be tracked and reported by federal agencies absent an Information Collection Request to indicate the extent of use of the Cybersecurity Framework in the Water Sector.

Objective 1

#### FINDINGS

People

* Community decision makers
* Executive management
* Water utility operators
* Cybersecurity staff

Utilities

* High existing capacity
  + Well equipped to implement the NIST Framework using existing tools, guidance, and resources
  + General to sophisticated understanding of cybersecurity principles
  + Have begun to implement cybersecurity measures
* Limited existing capacity
  + Little to no current adoption of cybersecurity measures
  + Require additional supporting resources to undertake implementation

To effectively promote use of the NIST Framework, we must:

* **Motivate** the Water Sector to take action to increase cybersecurity protections through:
  + Promoting basic awareness
  + Clear messaging around why implementation is important
  + Providing guidance on where information exists
* **Enable** the Water Sector to undertake activities to increase cybersecurity protections by providing:
  + Information that answers, *“How is the NIST Framework used?”*
  + Resources that support implementation and use

Training and outreach materials should:

* Use plain language and consistent terminology
* Be updated regularly
* Utilize existing delivery platforms (e.g., trainings, webcasts, websites)
* Support state primacy agency staff and technical assistance providers in their work with utilities

#### RECOMMENDATIONS

* Undertake an inventory review of existing training and outreach delivery platforms.
* Create an ongoing cybersecurity messaging campaign that is consistent across the Water Sector.
* Incorporate cybersecurity into the overall Water Sector culture. Identify 3-5 of the greatest opportunities for incorporating cybersecurity (e.g., continuing education programs).
* Provide sector-level threat briefings.
* Host training material on an open-source central portal.
* Host webinars and in-person trainings.

Objective 2:

#### FINDINGS

* A great deal of material exists to support the implementation and use of the Cybersecurity Framework, including:
  + AWWA *Process Control System Security Guidance for the Water Sector*
  + AWWA *Cybersecurity Guidance Tool*
* AWWA materials provide a “bridge” from the non-sector-specific NIST Framework to the Water Sector-specific user.
* Existing materials are sufficient to support implementation of the Framework by utilities with high existing cybersecurity capacity.
* Baseline level of knowledge of cybersecurity principles is required to implement NIST Framework and use supporting tools (e.g., AWWA tool and guidance) – not all utilities meet this baseline.

#### Recommendations

* Create business case materials to promote attentiveness to cybersecurity by decision makers.
* Create a simple language addendum to the AWWA guidance to help limited capacity utilities implement cybersecurity actions.
* Create an organizing framework for major resources. Should include a visual for how the resources relate to each other.
* Create educational materials specifically directed at state primacy agencies to help them better support low capacity utilities.
* Develop training and outreach directed at technical assistance providers to help them aid utilities in implementation.
* To assist technical assistance providers and directly support small and rural limited capacity utilities with enhancing cybersecurity, develop a simplified version of WaterISAC’s “10 Basic Cybersecurity Measures to Reduce Exploitable Weaknesses and Attacks.”
* Explore the opportunity represented by connecting the AWWA Tool and the CSET Tool to help improve user efficiency.

Objective 3:

#### Background

In developing the Objective 3 Recommendations, the workgroup took into account the new congressionally required GAO cybersecurity reporting requirements

Anticipated Uses of Cybersecurity Data:

* Understand the extent to which Water Sector utilities are aware of and have adopted cybersecurity voluntary standards and best practices.
* Use the information on adoption to understand the extent to which Water Sector utilities have taken risk management action to mitigate cybersecurity risk.
* Understand the factors that support and/or impede the adoption of voluntary cybersecurity standards and best practices in the Water Sector.
* Use the information on these factors to tailor sector outreach and training.
* Track changes in the cybersecurity risk profile at a national level over time to demonstrate improvements in response to sector outreach and training.

Needed Data to Support Anticipated Uses:

* Utility size (using standard categories such as those for SDWIS) and type (drinking water, wastewater, combined). Responding utilities will not be identified in survey results; participation will be anonymous.
* Utility awareness and use of cybersecurity guidance, tools, and resources, (e.g., NIST Cybersecurity Framework and AWWA Guidance).
* Utility cybersecurity implementation actions (addressed through limited number of actions)
  + Possibility of indicating the maturity of implementation.
  + Implementation actions and associated survey questions to correlate with Water Sector guidance (e.g., AWWA Guidance).
* Factors influencing utilities to adopt or not adopt cybersecurity voluntary standards and best practices.
* Data from responding utilities will be complimented with data collected by EPA and sector associations on the uptake of products related to cybersecurity outreach and training.

#### Recommendations

Survey Design Principles – *To confidently measure the adoption of cybersecurity best practices across the Water Sector, the assessment should strive to:*

* Prepare a compact, simple question structure
* Avoid introducing bias
* Obtain a sufficient sample size to confidently measure progress
* Stratify among known factors associated with cybersecurity adoption
* Maintain consistent survey instrumentation over time
* Be repeatable on a regular cycle (e.g., 2-year cycle)

Data Collection Implementation – *The Workgroup proposes the following approach to the collection of information on cybersecurity practices:*

* WSCC identifies Water Sector associations with an interest in voluntarily participating in data collection from their members
* EPA supports participating associations
* Two groups of SMEs will provide information:
  + Survey methods design
  + Survey questions design
* Associations independently determine final methods design and questions
* Associations participate consistently (e.g., implement a single survey)
* Associations or WaterISAC compile survey results and share aggregated results with EPA and other organizations that have a demonstrated need to know
* Data collection to be done with an awareness of, and potentially coordinated with, cybersecurity data collection efforts in other sectors