CIPAC Water Sector Cybersecurity Strategy Workgroup:

FINAL REPORT & RECOMMENDATIONS

April 2015

TABLE OF CONTENTS

Acronyms and Abbreviations

AWWA Guidance	American Water Works Association *Process Control System Security Guidance for the Water Sector*
C^3	Critical Infrastructure Cyber Community
CIPAC	Critical Infrastructure Partnership Advisory Council
CSET	Cyber Security Evaluation Tool
Cybersecurity Framework	*NIST Framework for Improving Critical Infrastructure Cybersecurity*
DHS	United States Department of Homeland Security
EPA	United States Environmental Protection Agency
FACA	Federal Advisory Committee Act
GAO	United States Government Accountability Office
GCC	Government Coordinating Council
NIST	National Institute of Standards and Technology
PCII	Protected Critical Infrastructure Information
SCC	Water Sector Coordinating Council
SDWIS	Safe Drinking Water Information System
SLTT	State, Local, Tribal, and Territorial
SME	Subject Matter Expert
Water Sector	Water and Wastewater Systems Sector
Workgroup	CIPAC Water Sector Cybersecurity Strategy Workgroup

Workgroup Background

The CIPAC Water Sector Cybersecurity Strategy Workgroup (Workgroup) was convened by the Water Sector Coordinating Council (SCC) and the Government Coordinating Council (GCC) to improve the resiliency of the Water and Wastewater Systems Sector (Water Sector) by developing a strategy to promote and facilitate use of the National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework). The Cybersecurity Framework provides a method that critical infrastructure owners and operators can use to create, assess, or improve comprehensive cybersecurity programs. The Workgroup was charged to accomplish the following three objectives.

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.

The Workgroup was comprised of twelve members, who represented large and small drinking water and wastewater systems, EPA, DHS, and other federal and SLTT agencies. Workgroup representatives were selected by the SCC and GCC. In addition, the Workgroup included two co-chairs; one selected by the SCC, and one from the EPA as the Sector Specific Agency for the Water Sector.

To address the three objectives, the Workgroup met twice in Washington, DC – once in August, 2014, and once in September, 2014. It engaged outside subject matter experts (SMEs) to provide supporting information and expertise related to the three objectives. Three task teams, consisting of Workgroup members, supporting staff, and SMEs, were also formed by the Workgroup – one to address each objective. These task teams met by phone.

The Department of Homeland Security exempted CIPAC and its workgroups (including the Water Sector Cybersecurity Strategy Workgroup) from the requirements of the Federal Advisory Committee Act (FACA).

Workgroup Findings

The findings included in this section represent observations that help to establish the context in which the Workgroup members have made their recommendations. The members believe that it is critical for the recommendations to be taken in context with the findings.

Cybersecurity Strategy Narrative

Throughout Workgroup discussions, an overarching strategy narrative emerged, describing the current condition of cybersecurity in the Water Sector, including use of the NIST Cybersecurity Framework, as well as the key elements of a strategy to increase use of the Cybersecurity Framework by the Water Sector.

The Workgroup has found that the Water Sector is currently well supported by tools and guidance that enable use of the Cybersecurity Framework. These tools and guidance deliver improvements in the overall cybersecurity posture of Water Sector utility participants. The most widely used Water Sector-specific resource for implementation of the NIST Framework is the AWWA Cybersecurity Guidance Tool (AWWA Tool) and the corresponding AWWA *Process Control System Security Guidance for the Water Sector* (AWWA Guidance). The AWWA Guidance provides a "bridge" from the non-sector specific NIST Cybersecurity Framework to the Water Sector-specific user. Despite the existing resources, to increase the adoption and use of the NIST Cybersecurity Framework, the Water Sector needs:

- **Increased motivation** to use the Cybersecurity Framework by increasing Water Sector knowledge of cybersecurity threats and demonstrating the business case (e.g., return on investment) for cybersecurity controls;
- **Enhanced capability** to implement the Cybersecurity Framework through increased technical and implementation support to Water Sector utilities, and increased support to assistance providers; and
- **A stronger cybersecurity culture** throughout the Water Sector that would encourage and support use of the Cybersecurity Framework, by embedding it as part of business as usual for utilities by improving the availability of information and lowering the cost of cybersecurity adoption.

Key Audiences

PEOPLE: There are four, key direct utility audiences for training and outreach efforts related to the Cybersecurity Framework:

(1) Community decision makers (such as elected officials and utility Board members);
(2) Executive management (including utility security managers);
(3) Water utility operators; and
(4) Cybersecurity staff (technical and professional staff, or those with cyber operations under their purview).

Effectively reaching these audiences to motivate support for cybersecurity attentiveness and NIST Framework use is critically important.

UTILITIES: Training materials and outreach campaigns related to the Cybersecurity Framework must tailor messaging, strategy, and delivery to two different Water Sector utility contexts: utilities with high internal information technology and cybersecurity capacity; and utilities with limited internal information technology and cybersecurity capacity. For both contexts, motivating two key actor categories (community decision makers such as elected officials and utility board members, and utility executive staff) to treat cybersecurity and the use of the NIST Framework as a priority is needed.

(1) High Existing Capacity: utilities with high existing capacity to address cybersecurity measures are well equipped to implement the cybersecurity framework using existing guidance, tools, and resources. They typically have a general to sophisticated understanding of cybersecurity principles and, at a minimum, have begun to implement cybersecurity measures. They range in size from small to large – capacity is not size dependent.

(2) Limited Existing Capacity: utilities with limited existing capacity are in the early stages of adoption, if at all, of cybersecurity measures, and typically lack the supporting resources needed to undertake such implementation. For utilities with limited in-house cyber capabilities, utility managers must still reach a basic level of understanding that allows them to manage contractors and consultants effectively. These utilities currently represent a majority of systems throughout the United States. They range in size from small to large – capacity is not size dependent.

Workgroup members believe it is important to note that there is also an additional subset of utilities, which have **very limited internal capacity**, and will never be able to implement cybersecurity protections without direct, hands-on technical assistance.

Workgroup Recommendations

Recommendations related to each of the three objectives are included in this section. Recommendations are accompanied by introductory background information, supporting text, and suggestions for responsible parties, where applicable.

Objective 1 Recommendations

OBJECTIVE 1 CHARGE: ***Develop approaches to outreach and training that will promote use of the Cybersecurity Framework by all segments of the Water Sector.***

BACKGROUND

To effectively promote use of the NIST Cybersecurity Framework, outreach and training approaches must address two key objectives:

1) **Motivate** the Water Sector to take action to increase cybersecurity protections through:
    a. Promoting basic awareness of the Cybersecurity Framework's existence, and
    b. Clear messaging around why implementation of the Cybersecurity Framework is important to utility functions and resilience.
2) **Enable** the Water Sector to undertake activities to increase cybersecurity protections by providing:
    a. Resources that support its implementation and use (addressed under Objective 2), and
    b. Guidance on where information exists for implementation of the Cybersecurity Framework (addressed under Objective 1).

The recommendations for approaches to outreach and training are organized around the two key objectives listed above. The Workgroup recommends that the implementation of each of the recommendations below follow these general principles:

- Training materials and outreach campaigns are designed to use plain language and consistent terminology that can be applied across the Water Sector.
- Training materials and outreach campaigns should be updated regularly, as cybersecurity principles are ever-changing with new technologies and practices.
- There are many existing delivery platforms (e.g., trainings, webcasts, websites), and a substantial volume of cybersecurity resources that can and should be leveraged. To the greatest extent possible, utilize these existing training and outreach delivery platforms by integrating cybersecurity messaging (both existing and new content) into them (e.g., integrated into existing all hazards resilience training and outreach).
- Recognize the role of state primacy agency staff and state-level utility technical assistance providers in supporting utilities, especially the more limited capacity systems, by creating training and outreach efforts to improve their capacity to promote and assist with implementation of the NIST Cybersecurity Framework.

RECOMMENDATIONS

*Specific recommendations are underlined, accompanied with descriptive text.

Recommendation 1.1 – Inventory of Existing Platforms	Undertake an inventory review of existing, potentially relevant training and outreach delivery platforms (e.g., trainings, webcasts, websites) of the Water Sector that can be leveraged to reach critical target audiences such as community decision makers, utility executives, and utility cyber staff. This inventory should take into account the intended audience(s) for each existing platform/resource, and should evaluate each platform's current scope and effectiveness in reaching its intended audiences. Undertaking this activity would support subsequent recommendations. SUGGESTED RESPONSIBLE PARTIES: • Lead party: EPA • Collaborators: DHS, associations, and state primacy agencies

MOTIVATE

Recommendation 1.2 – Core Messaging Campaign	Create an ongoing cybersecurity core messaging campaign, which is consistent across the Water Sector, and that targets utility managers, operators, and board members (this is a near-term/early action item, which would create a base for the subsequent recommendations). The messaging should be concise (e.g., similar to the "Stop.Think.Connect." or "Know Your Exposure" campaigns), highlight the Cybersecurity Framework, be applicable to the full range of system sizes and types, and leverage existing efforts (e.g., Cyber Security Awareness Month). Messaging should be shared through multiple sources and methods, including state and federal agencies, associations, through social media, websites, and direct outreach. SUGGESTED RESPONSIBLE PARTIES: • Lead Parties: Federal agencies (EPA, DHS) as lead developers • Collaborators: Associations and state primacy agencies.
Recommendation 1.3 – Incorporate Cybersecurity in the Water Sector Culture	Incorporate cybersecurity into the overall Water Sector culture (e.g., as a part of risk management). As a starting point, identify three to five of the greatest opportunities for incorporating cybersecurity. For example: (1) Including cybersecurity principles in security trainings, (2) Integrating cybersecurity concepts into the operator continuing education programs, and (3) Incorporating cybersecurity concepts into technical assistance provider site visits. SUGGESTED RESPONSIBLE PARTIES: • Lead party: EPA (leading the discussion) • Collaborators: DHS, associations, and states (specifically technical assistance providers and trainers).

Recommendation 1.4 – Sector-Level Threat Briefings	Explore opportunities for additional venues to provide sector-level threat briefings with the objective of driving broader awareness of cybersecurity threats, similar to the current Water ISAC briefings (e.g., WARNs, PSA). Additionally, create more generic declassified briefings that are tailored to the Water Sector audience and context. SUGGESTED RESPONSIBLE PARTIES: • Lead Party: DHS • Collaborators: WaterISAC, EPA, and other associations

ENABLE

Recommendation 1.5 – Open Source Portal for Training Materials	Host all training material relevant to the Cybersecurity Framework on an open-source central portal (e.g., WaterISAC). Promote this centralized resources portal on all websites where Water Sector utilities may turn for cybersecurity information (e.g., EPA, DHS, associations, and state agency websites). As an independent section of training materials, collect and enable sharing of best practices (case examples) related to implementation of the Cybersecurity Framework at Water Sector utilities (e.g., through a Water Sector collaborative partnership on cybersecurity similar to the Effective Utility Management model, using websites, social media, and newsletters). Best practices should be focused on Cybersecurity Framework implementation tactics, updated regularly, and selected using a standardized filter to control content and volume. SUGGESTED RESPONSIBLE PARTIES: • Lead Party: Water ISAC • Collaborators: Federal agencies (EPA, DHS), associations, state agencies, and Water Sector participants (e.g., managers and operators).
Recommendation 1.6 – Host Trainings	Host webinars and in-person trainings to address the following: (1) The AWWA Guidance and its uses, (2) Introduction to the Cybersecurity Framework and its applicability to Water Sector, (3) Basic implementation tips for the Cybersecurity Framework at Water Sector utilities, and (4) An overview of significant tools and resources available to assist in implementation of the Cybersecurity Framework. SUGGESTED RESPONSIBLE PARTIES: Federal agencies (EPA headquarters, EPA regions, EPA Office of Research and Development, and DHS), in conjunction with WaterISAC, associations, and state agencies.

Objective 2 Recommendations

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

BACKGROUND

The Workgroup has identified the following findings related to gaps in resources that exist to support the use and implementation of the NIST Cybersecurity Framework:

- **FINDING 1:** A great deal of material exists to support the implementation and use of the Cybersecurity Framework, including the AWWA Guidance and the AWWA *Cybersecurity Guidance Tool*. Overall, existing guidance, tools, and resources appear sufficient to support implementation and use of the NIST Cybersecurity Framework by utilities with high cybersecurity capacity.
- **FINDING 2:** A baseline of knowledge of cybersecurity imperatives and fundamentals is required to implement the Cybersecurity Framework and use the existing supporting tools (e.g., the AWWA Guidance). Water Sector utilities must each reach this general level of baseline knowledge to be able to effectively use the tools and resources that currently exist. Utilities also often engage external contractors for IT and cybersecurity support. It is important that they be equipped with a sufficient understanding of cybersecurity principles to allow them to effectively communicate with and manage these contractors.

Recommendations related to the gaps in existing guidance, tools, and resources are designed in support of these key findings.

RECOMMENDATIONS

*Specific recommendations are underlined, accompanied with descriptive text.

Recommendation 2.1 – Business Case Materials for Decision Makers	A gap exists in resources that are designed to help motivate key decision makers (e.g., elected officials, water utility board members, and utility executive management) to support implementation of the Cybersecurity Framework and other cybersecurity measures. This gap applies to the full range of utilities from high to limited capacity, and can be filled by creating materials that make a business case for cybersecurity measures and highlight the risks associated with not implementing these measures. Short, pointed cybersecurity business case materials (e.g., fact sheets, general tips, primers) specifically tailored to the Water Sector should be developed that are designed to educate and promote attentiveness to cybersecurity needs by decision makers. These materials should be written in cybersecurity language that has been standardized across the Water Sector, and should answer the question, "Why should Water Sector utilities be interested in cybersecurity practices?" Department of Homeland Security's *Cyber Risk Management Primer for CEOs* and other related resources can be tailored/leveraged to be Water Sector-specific to fit these purposes. Materials should also include background information on the Cybersecurity Framework, such as why it was created and what it was designed to do.

Recommendation 2.2 – Simple Language Addendum to AWWA Guidance	A gap exists in current guidance, tools, and resources that cover basic cybersecurity principles for Water Sector utilities with limited capacity for implementation of the Cybersecurity Framework (note that this recommendation is geared specifically toward those charged with cybersecurity implementation, distinct from Recommendation 2.1, which is geared toward decision makers). This gap can be filled by creating a simple-language version of the twelve practice categories listed in the AWWA Guidance to help utilities (specifically limited capacity utilities) implement cybersecurity actions in conformance with the basic Cybersecurity Framework implementation expectations. The document should also include:
	• Information to provide knowledge and awareness of basic cybersecurity principles through fundamental questions that give utilities better situational awareness related to their current capacity and better equip limited capacity utilities to use the AWWA Guidance and Tool
	• Basic cybersecurity principles:
	  ○ Tactical basics (e.g., using passwords)
	  ○ Programmatic basics (e.g., the building blocks of an effective cybersecurity program)
	• Background information on the Cybersecurity Framework:
	  ○ Why it was created
	  ○ What it is designed to do
	  ○ A basic checklist for Cybersecurity Framework implementation
	• A clearly organized compilation of available guidance, tools, and resources to support implementation of the Cybersecurity Framework
	• A path to approach continual cybersecurity improvement that supports utilities who want to move past the basics. This path would connect to the AWWA Guidance
	• Basic implementation checklist(s) for the AWWA Guidance and the Cybersecurity Framework
	
	This material would not serve as a new tool or a second version of the AWWA Guidance. It would serve as a supplemental addendum to the AWWA Guidance to help increase the usability and accessibility of the Guidance, particularly to limited capacity systems.

Recommendation 2.3 – Organizing Framework for Major Resources	A gap exists related to the organization and accessibility of current guidance, tools, and resources. High capacity Water Sector utilities would be the primary audience, and would benefit from an organizing framework for all resources related to the Cybersecurity Framework and other cybersecurity measures. This framework should include a simple graphic or other visual representation of how the major resources relate to each other or nest with each other, their topical scopes, and which user groups they are intended for. Major resources to be included in this framework should include, but not be limited to: AWWA's Guidance and *Cybersecurity Guidance Tool*, Department of Homeland Security's Critical Infrastructure Cyber Community (C^3) Voluntary Program and Cyber Security Evaluation Tool (CSET) programs, and the SANS Institute Critical Security Controls. The framework would lower the transaction cost for utilities associated with working through how the current resources fit together when implementing the Cybersecurity Framework.

Recommendation 2.4 – Education Materials for State Agencies	A gap exists in the resources available to state primacy agencies related to implementation of the Cybersecurity Framework. State primacy agencies are not currently well equipped to play a supporting role to their typical audience (generally the very low capacity utilities) in implementing cybersecurity measures. This gap can be filled by creating educational materials directed specifically at the state primacy agencies to help them better support low capacity utilities in implementing the Cybersecurity Framework. These materials must reflect that the current business case available to the Water Sector is failing to motivate utilities to make investments of the right type at the right time. Additionally, the materials should reflect that an important dimension of cybersecurity success is the organizational policy and personnel engagement. By providing state agencies with this information, these agencies can then help to motivate their Water Sector utility constituencies to implement cybersecurity measures, including the Cybersecurity Framework.
Recommendation 2.5 – Training and Outreach Materials for Technical Assistance Providers	A gap exists in the resources available to technical assistance providers related to implementation of the Cybersecurity Framework. This gap can be filled by developing targeted training and outreach for technical assistance staff that will enable them to provide Water Sector utilities with essential information to promote and aid in implementation of the Cybersecurity Framework. Additionally, to assist technical assistance providers and directly support small and rural limited capacity utilities with enhancing cybersecurity, the Workgroup recommends the development of a simplified version of WaterISAC's "10 Basic Cybersecurity Measures to Reduce Exploitable Weaknesses and Attacks." This product should include a "Have you done these steps?" type of checklist that is designed to inform the small and rural system user about cybersecurity improvement needs and options, as well as establish a list of cybersecurity actions for implementation at the utility. Creating stronger support for these technical assistance providers and small and rural systems will help to create a more complete cybersecurity implementation, especially for those small and rural low cybersecurity capacity utilities that lack the financial resources to acquire private consulting services and are challenged to implement cybersecurity protections without additional assistance.
Recommendation 2.6 – Explore Integrating AWWA Tool with CSET	Explore the opportunity represented by connecting the AWWA Tool to CSET to improve efficiency of use by Water Sector utilities seeking to move beyond basic implementation.

Objective 3 Recommendations

OBJECTIVE 3 CHARGE: ***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.***

PART 1: INFORMATION NEEDS DESCRIPTION

Objective 3 of the Water Sector Cybersecurity CIPAC Charter states that the CIPAC Workgroup will: "seek to identify measures of success that indicate the extent of use of the Cybersecurity Framework in the Water Sector. It is anticipated that federal agencies (including DHS and EPA) and Water Sector associations will use these measures of success to evaluate the effectiveness of outreach and training efforts, as well as the adequacy of guidance, tools, and resources, for achieving widespread adoption of the NIST Cybersecurity Framework in the Water Sector. EPA does not expect to have an Information Collection Request to support collection of this information. Accordingly, EPA cannot gather information on Cybersecurity Framework usage through surveys."

In addition, the Cybersecurity Enhancement Act of 2014 (enacted December 18, 2014) requires the Government Accountability Office (GAO) to submit regular reports to Congress on the extent to which federal agencies have promoted and critical infrastructure sectors have adopted voluntary standards to reduce cyber risks, the reasons behind the decisions of critical infrastructure sectors to adopt or not adopt the voluntary standards, and the extent to which such voluntary standards have proved successful in protecting critical infrastructure from cyber threats. Based on past practice, GAO is expected to request the information on the Water Sector needed for these reports from EPA, the WSCC, and sector associations.

Within the context of this background, the CIPAC Water Sector Cyber Strategy Workgroup recommends that, upon approval of its final report, the WSCC lead Water Sector associations in the collection of information on cybersecurity practices in the Water Sector and related measures, as described below.

1. **Uses of Cybersecurity Data:**
    a. To understand the extent to which Water Sector utilities are aware of and have adopted cybersecurity voluntary standards and best practices.
    b. To use the information on adoption to understand the extent to which Water Sector utilities have taken risk management action to mitigate cybersecurity risk.
    c. To understand the factors that support and/or impede the adoption of voluntary cybersecurity standards and best practices in the Water Sector.
    d. To use the information on these factors to tailor sector outreach and training.
    e. To track changes in the cybersecurity risk profile at a national level over time to demonstrate improvements in response to sector outreach and training.

2. **Needed Data:**
    a. Responding utilities will indicate size (using standard categories such as those for the Safe Drinking Water Information System – SDWIS) and type (drinking water, wastewater, combined). Responding utilities will not be identified in survey results; participation will be anonymous.
    b. Responding utilities will indicate awareness and use of cybersecurity guidance, tools, and resources, such as the NIST Cybersecurity Framework and AWWA Guidance, by selecting from a list.
    c. Responding utilities indicate their cybersecurity implementation actions, with the possibility of indicating the maturity of implementation if the survey design can address the subjective nature of

reporting on maturity levels. The implementation actions and associated survey questions are expected to correlate with Water Sector guidance on cybersecurity voluntary standards and best practices, such as the AWWA Guidance.

d. Responding utilities select factors from a limited list that have influenced their decisions to adopt or not adopt cybersecurity voluntary standards and best practices.
e. 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.

PART 2: SURVEY DESIGN PRINCIPLES

Survey design and implementation methods must support making statistically valid inferences about Water Sector progress, with an emphasis on direct Water Sector utility information, including water and wastewater utilities ranging in size from small to large.

To confidently and validly generalize self-report survey results to the entire Water Sector, survey respondents representative of the broader water utility population are needed. The sample of water utilities that complete surveys should also be a sufficient size to estimate the prevalence of feedback responses with adequate precision. There are a variety of potential biases that could influence survey results (particularly in the area of cybersecurity), and that survey design will need to manage for. For example, a low response rate may indicate a selection bias wherein utilities with known cybersecurity weaknesses are less likely to respond than utilities that are confident in their cybersecurity preparedness. Additionally, time and resource availability can impact the response rate; insufficient staff capacity (at organizations administering the survey) to conduct the follow-up typically needed to produce a representative response would leave gaps in the target response pool. To confidently measure the adoption of cybersecurity best practices across the Water Sector, the assessment should strive for the following:

1. **Prepare a compact, simple question structure.** To support survey participant willingness to complete the survey, the design should strive for a limited number of straightforward questions that can be answered quickly and easily. An overly complex and detailed design will be challenging to complete and create disincentives to participate in the survey effort.

2. **Avoid introducing bias.** To avoid introducing bias, respondents should be from a random sample of the sector with a high survey response rate. If this cannot be achieved, it should be statistically demonstrated that the respondents and non-respondents are not characteristically different (e.g., representing different utility sizes). Survey design should also seek to accommodate the potential for a less than optimal response rate, while still supporting reasonable confidence in the interpretation and application of results to Water Sector conditions (e.g., the survey could include questions that can inform the type of bias, if any, that may be present in the actual survey respondent pool).

3. **Represent the broader Water Sector.** If the survey is administered to a sample of the sector, this sample should be representative of all utilities. For example, if the survey is administered at a conference, the study designers should be confident that the attendees are representative of all utilities, and not simply those that had resources to send staff to the conference.

4. **Obtain a sufficient sample size to confidently measure progress.** Sample size calculations should be conducted prior to distributing the assessment to ensure adequate statistical power to measure progress and avoid incorrect inferences as a result of random variability.

5. **Stratify among known factors associated with cybersecurity adoption.** If a factor such as utility size has been previously demonstrated to be associated with adopting best practices, statistical analysis should include methods to adjust for the role of utility size and other known factors on cybersecurity adoption (e.g., standardization, stratification). Utility size is likely a particularly important aspect of stratification in light of the substantial imbalance in the number of systems spread across the small, medium, and large water system spectrum.

6. **Maintain consistent survey instrumentation.** To measure the success of the program over time, the survey must maintain the same questions between assessment periods. Questions can be added or removed, but comparisons across assessments must be of the same question.

The survey should be repeatable on a regular cycle (e.g., 2-year cycle) to demonstrate progress over time. A baseline should be established as soon as possible to provide a firm foundation for measuring progress over time.

PART 3: DATA COLLECTION IMPLEMENTATION

As stated in Part 1, the CIPAC Water Sector Cyber Strategy Workgroup recommends that, upon approval of its final report, the WSCC lead Water Sector associations in the collection of information on cybersecurity practices in the Water Sector and related measures. The Workgroup proposes the following approach to the collection of information on cybersecurity practices.

1. The Workgroup recommends that the WSCC identify Water Sector associations with an interest in voluntarily participating in the collection of data from their members on the awareness and use of cybersecurity guidance, tools, and resources, and the adoption of cybersecurity voluntary standards and best practices.

2. The Workgroup recommends that EPA support participating Water Sector associations by making subject matter experts (SMEs) available to work collaboratively with the associations on two tasks:
    a. One group of SMEs will provide information to assist the design of the Water Sector cybersecurity surveys (e.g., methods to determine the number of water utilities to be queried and target response rates in different size ranges; how to develop QA/QC for compiling survey responses);
    b. A separate group of SMEs will provide information to assist the design of the cybersecurity survey questions (e.g., identify the specific cybersecurity practices to be addressed).

    EPA should support the work of the SMEs as required.

3. The Workgroup understands that the participating Water Sector associations must independently determine the final Water Sector cybersecurity survey design and questions after receiving information from and working collaboratively with the SMEs.

4. To support the ability to confidently interpret results across all participating associations, the Workgroup recommends that the WSCC foster consistent participation by Water Sector associations. This includes implementing a single survey with an explicitly accepted design, conducted on the same timeframe, and using comparable random response validation efforts and response analysis protocols. The Workgroup recommends the Water Sector associations develop and agree to a joint plan to support this consistency. The Workgroup anticipates that executing the surveys will involve the associations sending surveys to appropriate points of

contact at a limited number of water or wastewater utilities, and then conducting follow-up as required to achieve the target response rate, recognizing that certain factors such as resource constraints and the ability to obtain needed contact information may constrain fully meeting the target response rate.

5. The Workgroup recommends that participating Water Sector associations or WaterISAC compile survey results in accordance with survey design QA/QC and, in a timely manner, share aggregated results with EPA and other organizations that have a demonstrated need to know. The aggregated results could potentially be designated as Protected Critical Infrastructure Information (PCII). The Workgroup anticipates that EPA will not have access to individual survey responses.

6. The Workgroup recommends that the collection of data on cybersecurity in the Water Sector be done with an awareness of, and potentially coordinated with, cybersecurity data collection efforts in other critical infrastructure sectors. For example, insurers with the Financial Services Sector have recently developed cyber-insurance products, and their uptake in the Water Sector could act as one indicator of increased attentiveness to cybersecurity needs and risks. There are also additional questions to answer as part of designing the process for survey development, including:
    a. If the Water Sector associations alter the survey as designed in collaboration with the SMEs, what process will be used to ensure the intended validity of the survey is preserved?
    b. What process will be used to reach agreement on final survey design and implementation among the Water Sector associations, and how will any failure to reach agreement be managed to avoid a substantial setback to understanding Water Sector cybersecurity progress?
    c. Can the survey design and implementation approach accommodate States' interest to better inform their technical assistance and training efforts, while maintaining a short, focused survey and protecting the anonymity of survey respondents?

Conclusion

The CIPAC Water Sector Cybersecurity Strategy Workgroup has concluded that the Water Sector is currently well supported by tools and guidance that enable use of the Cybersecurity Framework. These tools and guidance deliver improvements in the overall cybersecurity posture of the Water Sector. However, despite the existing resources, the Water Sector would benefit from additional resources and actions at the federal, state, and association levels.

The Workgroup has found that to increase the adoption and use of the NIST Cybersecurity Framework, the Water Sector needs:

- **Increased motivation** to use the Cybersecurity Framework by increasing Water Sector knowledge of cybersecurity threats and demonstrating the business case (e.g., return on investment) for cybersecurity controls;
- **Enhanced capability** to implement the Cybersecurity Framework through increased technical and implementation support to Water Sector utilities, and increased support to assistance providers; and
- **A stronger cybersecurity culture** throughout the Water Sector that would encourage and support use of the Cybersecurity Framework, by embedding it as part of business as usual for utilities by improving the availability of information and lowering the cost of cybersecurity adoption.

Furthermore, the Workgroup has found that the key audiences to target for uptake of these materials are:

- **People**, including community decision makers, executive management, water utility operators, and cybersecurity staff; and
- **Utilities**, including utilities with high internal information technology and cybersecurity capacity; and utilities with limited (and very limited) internal information technology and cybersecurity capacity.

The Workgroup proposes that activities at the federal, state, and association level, which are detailed in the Recommendations section of this report, will help to fill the existing gaps and inform cybersecurity activities and needs in the Water Sector going forward. Finally, to track sector progress and understand how resources, trainings, and outreach can be improved over time, the Workgroup recommends the development and administration of a survey by Water Sector associations that would provide a better understanding of the extent to which Water Sector utilities are aware of and have adopted cybersecurity voluntary standards and best practices.

CIPAC Water Sector Cybersecurity Strategy Workgroup: Final Report & Recommendations