**Documents for the Record**

**E&C Oversight Hearing 5.16.23**

**"Protecting Critical Infrastructure from Cyberattacks: Examining Expertise of Sector Specific Agencies"**

1. American Water Works Association Letter to the United States Conference of Mayors Regarding Renewal of Public Water System Supervision Program
2. Joint Letter to State Drinking Water Administrators on Public Water System Cybersecurity
3. Joint Letter to EPA and ICR Regarding Cybersecurity Rule
4. Joint Sanitary Survey Letter to EPA
5. Letter from American Public Power Association regarding the cyber security hearing.

## 1) American Water Works Association Letter to the United States Conference of Mayors Regarding Renewal of Public Water System Supervision Program

***VIA ELECTRONIC SUBMISSION***

**RE: Agency Information Collection Activities; Submission to the Office of Management and Budget for Review and Approval; Comment Request; Public Water System Supervision Program (Renewal), EPA-HQ-OW-2011-0443**

Dear Administrator Regan and Administrator Revesz,

The American Water Works Association ("AWWA") and the US Conference of Mayors ("US Mayors") are filing comments on the U.S. Environmental Protection Agency ("EPA") request for comments on the proposed renewal of the Information Collection Request ("ICR") for the Public Water System Supervision Program ("PWSS"). These comments reflect the lack of coverage for the Cyber Rule issued by EPA on March 3, 2023,[1] and assumptions associated with existing and future burden assessment.

The ICR for the PWSS Program (ICR No. 2040-0090) covers information collections for "General State Primacy Activities" to implement compliance oversight and enforcement responsibilities under the Safe Drinking Water Act ("SDWA") which includes obligations for the primacy agency to maintain records on the results of sanitary surveys per 40 CFR 142.14.

[1] PA, March 3, 2023, *Addressing PWS Cybersecurity in Sanitary Surveys or an Alternate Process* ("Cyber Rule")

As highlighted previously,[2] EPA has a statutory obligation under the Paperwork Reduction Act ("PRA") to assess the burdens associated with the mandatory information collection and recordkeeping requirements created by the Cyber Rule. An ICR extension does not allow for the addition or inclusion of new information collection and recordkeeping requirements. Further the information collection requirements associated with the new Cyber Rule do not exist within the current sanitary survey program.

If cybersecurity was indeed part of the current sanitary survey program, there would be no need for EPA to issue the Cyber Rule and supporting guidance. As a point of reference, the terms "cyber" and "internet" do not even appear in EPA's current sanitary survey guidance.[3] Since it is not included, EPA is required by the PRA and regulations controlling paperwork burdens on the public to publish an ICR for public review and comment. In the absence of an approved ICR, state primacy agencies are not authorized to collect this information and public water systems are not required to respond to requests for information.

AWWA and the US Mayors recognize that the burden associated with a public water system responding to a sanitary survey is covered in multiple ICRs that have been approved individual SDWA regulations and not the PWSS Program. Typically, EPA states that the "PWS burden also includes the burden associated with sanitary surveys" but the expected burden of responding to the new sanitary survey requirements in the Cyber Rule, including minimum expected hours, have not been assessed by the agency. In addition, none of the following ICRs that include sanitary survey obligations address the new information collection and recordkeeping requirements created by the Cyber Rule:

- Microbial Rules (ICR No. 2040-0205)
- Lead and Copper Rule Revisions (ICR No. 2040-0297)

- Disinfectants/Disinfection Byproducts, Chemical and Radionuclides (ICR No. 2040-0204)

The only substantive analysis of the burdens associated with performing and responding to sanitary surveys by states and public water systems is the 2006 *Economic Analysis for the Final Ground Water Rule*,[4] which estimated labor cost and hours for the following sanitary survey activities:

- Review/Inspect Wells (State & PWS)
- Review/Inspect Treatment (State & PWS)
- Review/Inspect Distribution System (State & PWS)
- Report Review and Discussion (State & PWS)
- Report Documentation/File Review (State)
- Report Development (State)
- Date Entry (State)
- Travel (State)

[2] Letter dated March 17, 2023 to EPA Administrator Regan and OIRA Administrator Revesz from the American Water Works Association, Association of Metropolitan Water Agencies, National Association of Water Companies and The United States Conference of Mayors (attached)
[3] USEPA 2019, Sanitary Survey Field Reference for Use When Conducting a Sanitary Survey of a Small Water System, EPA 816-R-17-002
[4] USEPA 2006, Economic Analysis for the Final Ground Water Rule, EPA 815-R-06-014



The burden obligations in the following tables represent some of the new information collection and recordkeeping obligations for states and public water system based on the Cyber Rule. The 2006 sanitary survey analysis should be used as a template for an ICR to capture the new burden obligations.

**States**

| Information & Recordkeeping Activity | Changes in Burden Obligation |
|---|---|
| *Familiarization with the new Cyber Rule* | EPA has developed a 6-hour training for states to support this need |
| *Assessing cybersecurity during sanitary survey* | EPA has estimated the additional time required for states to assess cybersecurity based on population served by the system[5]<br>• 2 hours (less than 50,000)<br>• 4 hours (50,000 – 100,000)<br>• 6 hours (greater than 100,000) |
| *Recordkeeping*<br>• Track cyber assessment status<br>• Document deficiencies, including significant deficiencies requiring corrective action<br>• Track corrective actions | Currently state databases used to track and record results of sanitary survey do not include data fields designed to track compliance with cybersecurity provisions detailed in EPA guidance, which include 33 controls that may be assessed. |

**Public Water Systems**

| Information & Recordkeeping Activity | Changes in Burden Obligation |
|---|---|
| *Familiarization with the new Cyber Rule* | EPA has provided 6-hour training for PWS to support this need[6] |

| | |
|---|---|
| *Assessing cybersecurity during sanitary survey* | The time EPA estimated the state will be on site for the cyber assessment will also be incurred by the PWS.<br><br>In addition, the PWS will expend time to prepare the documentation necessary to demonstrate compliance with specific cyber controls. This may also require capitol investments to address controls that EPA has identified as potential "significant deficiencies".<br><br>EPA's checklist includes 33 controls that they assert are "technically feasible for most PWS to address without significant capital expenditures", however EPA has not provided any documentation that characterizes how this determination was made. |

[5] USEPA, March 16, 2023, Cybersecurity Assessment Training for Primacy Agencies: Part One and Part Two
[6] USEPA, March 9, 2023, Cybersecurity Assessment Training for Public Water Systems: Part One and Part Two



| | |
|---|---|
| | Using EPA's checklist and related training as a baseline, the Rule requires assembling an often-complex set of information sources to document compliance and in some cases may be difficult for the state to authenticate. |
| *Recordkeeping*<br>• Document conformity, including significant deficiencies requiring corrective action<br>• Track corrective actions<br>• Report deficiencies on annual Consumer Confidence Report<br>• Copies of any written reports, summaries, or communications relating to sanitary surveys must be retained for 10 years. | Results of the sanitary survey requiring corrective action in many instances may require capital expenditures to mitigate. A deficiency may also require public notice as part of the Consumer Confidence Report. |

We again respectfully ask that EPA withdraw the Cyber Rule until such time that it has fulfilled the statutory obligations defined by the PRA and regulations controlling paperwork burdens on the public. In addition, OMB should provide a statement clarifying that any information collected to support compliance with the Rule would constitute a violation of the PRA and regulations controlling paperwork burdens on the public. We have further concerns with the lack of legally-required procedures followed before issuing the Cyber Rule which we look forward to addressing with both the agency and OMB.

Sincerely,

American Water Works Association
The US Conference of Mayors

cc: Janet McCabe – EPA/OA
Radika Fox – EPA/OW
Tim DelMonico – EPA/OCIR
Vicki Arroyo – EPA/OP
Jeffrey Prieto – EPA/OGC
Sean O'Donnell – EPA/OIG
Jennifer McLain – EPA/OW/OGWDW
David Travers – EPA/OGWDW/WICRD



March 17, 2023

Mr. Michael Regan
Administrator
U.S. Environmental Protection Agency
1200 Pennsylvania Ave, NW
Washington, DC 20460

Mr. Richard Revesz
Administrator
Office of Information and Regulatory Affairs
1650 Pennsylvania Avenue, NW
Washington, DC 20503

**RE: Public Water System Supervision Program (ICR No. 2040-0090)**

Dear Administrator Regan and Administrator Revesz,

The undersigned associations write to you regarding the March 3, 2023 agency action issued by the U.S. Environmental Protection Agency ("EPA") to State Drinking Water Administrators entitled "*Addressing PWS Cybersecurity in Sanitary Surveys or an Alternate Process*" (the "Rule"), which requires states to examine cybersecurity practices and controls at public water systems ("PWS") while conducting sanitary surveys and collect data from PWS regarding the same. This is one of several new substantive requirements imposed by EPA's new final Rule. According to EPA, this Rule is effective immediately. However, the information collection and record keeping requirements associated with this new Rule violate the Paperwork Reduction Act ("PRA") and are not covered by EPA's current Information Collection Request ("ICR") for the Public Water System Supervision Program ("ICR No. 2040-0090"). This ICR covers information collections for "General State Primacy Activities" to implement compliance oversight and enforcement responsibilities under the SDWA. This includes requirements for the primacy agency to maintain records such as the results of sanitary surveys per 40 CFR 142.14. ICR No. 2040-0090 expires on March 31, 2023.[1]

[1] Notice of Office of Management and Budget Action, Public Water System Supervision Program (EPA ICR No. 0270.47), Issued 3/09/2020, https://www.reginfo.gov/public/do/PRAViewICR?ref_nbr=201903-2040-005#

Given the absence of an OMB approved ICR for the information required under the new Rule, state primacy agencies are not authorized to collect this information and public water systems are not required to respond to requests for information.

More specifically, Congress made it very clear in the PRA[2] that an agency shall not conduct or sponsor the collection of information unless in advance of the adoption or revision of the collection of information, the agency has completed all requirements provided in OMB regulations for data collection.[3] This includes publishing a notice in the Federal Register that provides the following:

- a title for the collection of information;
- a summary of the collection of information;
- a brief description of the need for the information and the proposed use of the information;
- a description of the likely respondents and proposed frequency of response to the collection of information;
- an estimate of the burden that shall result from the collection of information;
- notice that comments may be submitted to the agency and OMB; and
- the time period within which the agency is requesting OMB to approve or disapprove the collection of information.

The agency has not fulfilled its obligation to assess burdens the Rule will impose on primacy authorities or PWSs. The Rule requires the collection and review of substantively new and different information than what is currently approved in the current ICR. While the agency's Rule did undergo E.O. 12866 review, no new supporting statement or revised ICR has been prepared or issued for public review and comment.

We are not aware that EPA has given public notice to support renewal of this ICR, that would include providing revised burden estimates, and published a justification of the practical utility of the ICR requirements, especially those contained in the new Rule. Examples of new requirements for primacy agency and PWSs that result in burdens due to the Rule include, but are not limited to, the following:

*Training*[4]

- EPA has released 6 hours of training for states to review the Rule, implementation options and available resources. The training includes a table provided by EPA estimating "*the additional time required for states to assess cybersecurity will be reflective of the population served by the system*."

[2] Paperwork Reduction Act, Public Law 104-13, https://www.reginfo.gov/public/reginfo/pra.pdf
[3] 5 CFR 1320 - Controlling Paperwork Burdens on the Public, https://www.govinfo.gov/content/pkg/CFR-2010-title5-vol3/xml/CFR-2010-title5-vol3-part1320.xml
[4] EPA Cybersecurity for the Water Sector – Training, https://www.epa.gov/waterriskassessment/epa-cybersecurity-water-sector#rule

- EPA has released 6 hours of training for PWSs demonstrating how to use EPA's cybersecurity checklist to assess their program, information on how to address vulnerabilities, and available resources. EPAs checklist includes 33 questions related to various cybersecurity controls for which no estimated time burden is provided, but a majority are classified in the training materials as potential "significant deficiencies" if not implemented.

*Recordkeeping*

- States must maintain records of significant deficiencies and confirmation that the deficiency has been corrected. This requires a modification of existing compliance data systems to add necessary data fields to document cybersecurity related items as part of the sanitary survey.
- States must develop and maintain list of "approved agents" if it allows agents other that the state to conduct the cybersecurity component of the sanitary survey.
- States must add cybersecurity to their annual evaluation of the state's program for conducting sanitary surveys in the report transmitted to EPA.

*Expanded Scope of Coverage*

- EPA records[5] indicate that there are 151,606 PWSs for which this Rule may apply. According to EPA compliance records there are 10,003 community water systems that serve 3,300 or more persons that must comply with AWIA §2013.[6] These systems are mandated by Congress to include an assessment of cybersecurity threats as part of a risk and resilience assessment and an emergency response plan. Therefore, the scope of the Rule captures an additional 141,603 PWSs that would at minimum be required to assess the applicability of the new Rule and associated requirements.

We do not believe that the expiration of the current ICR satisfies any of the criteria that may justify emergency processing by OMB. There is no reasonable explanation for why the agency would be unable to comply with the normal clearance procedures for the existing ICR. The addition of new information collection obligations created by the Rule do not justify emergency processing either since this action has been under consideration by the agency since 2021.[7] Finally, there has been no consultation or collaboration with the organizations

[5] EPA, Safe Drinking Water Information System (SDWIS), 2022Q4 Summary Data
[6] EPA, America's Water Infrastructure Act Section 2013 Compliance Data, https://www.epa.gov/waterresilience/americas-water-infrastructure-act-section-2013-compliance-data
[7] Unified Agenda of Regulatory and Deregulatory Actions, Fall 2021, https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202110&RIN=2040-AG20

representing PWSs regarding considerations that might "minimize the burden" per 5 C.F.R. 1320.13.

Respectfully, we ask that EPA withdraw the Rule until such time that it has fulfilled the statutory obligations defined by the PRA and regulations controlling paperwork burdens on the public. In addition, OMB should provide a statement clarifying that any information collected to support compliance with the Rule would constitute a violation of the PRA and regulations controlling paperwork burdens on the public. We have further concerns with the lack of legally-required procedures followed before issuing the Rule which we look forward to addressing with both the agency and OMB.

Sincerely,

American Water Works Association
Association of Metropolitan Water Agencies
National Association of Water Companies
US Conference of Mayors

cc: Radika Fox – EPA/OW
Tim Del Monico – EPA/OCIR
Vicki Arroyo – EPA/OP
Jeffrey Prieto – EPA/OGC
Sean O'Donnell – EPA/OIG
Jennifer McLain – EPA/OW/OGWDW
vers – EPA/OGWDW/WICRD

2) Joint Letter to State Drinking Water Administrators on Public Water System Cybersecurity

January 25, 2023

Mr. Michael Regan
Administrator
Environmental Protection Agency
1200 Pennsylvania Ave, NW
Washington, DC 20460

**Re: Pending EO 12866 Regulatory Review: Memorandum to State Drinking Water Administrators on Public Water System Cybersecurity**

Dear Administrator Regan,

The undersigned associations write you regarding EPA's Memorandum to State Drinking Water Administrators on Public Water System Cybersecurity, which OMB is currently reviewing.

Collectively we are dedicated to protecting public health and the environment by providing safe drinking water and excellent wastewater services. The infrastructure our members maintain is the foundation on which U.S. communities are built.

Cybersecurity is mission-critical for all types of water utilities. As such, we support efforts to strengthen cybersecurity, and are eager to collaborate with the agency to develop and implement effective approaches. However, EPA's planned efforts to add cybersecurity requirements to the Sanitary Survey Program for drinking water utilities are ill-advised, impractical, and are not designed to meaningfully improve system resiliency. EPA's approach is also legally flawed as described in the addendum to this letter.

We write to raise the significant legal, procedural, and policy concerns drinking water utilities have regarding the imposition of cybersecurity requirements through the Sanitary Survey

Program and offer a process to examine alternatives. Ultimately, we fear the Sanitary Survey approach could do more harm than good for drinking water utilities.

To that end, we are committed to working collaboratively with EPA and other stakeholders to develop an effective approach to cybersecurity that is risk- and performance-based. We recognize the necessity to act, and we are committed to working expediently to develop and implement cybersecurity solutions for the water sector that are developed by consensus with critical input and support from water utilities, an approach that is legally sound and will result in a far more effective approach to mitigate cyber threats facing the water sector.

Thus, to best serve our shared goal of cybersecurity solutions for the water sector, we urge you to recall the RIN 2040-ZA41 Memorandum under review at the Office of Management and Budget for reconsideration with stakeholders and to ensure compliance with all applicable laws.

Sincerely,

American Water Works Association
Association of Metropolitan Water Agencies

National Association of Clean Water Agencies
National Association of Counties
National Association of Water
Companies National League of Cities
National Rural Water Association
US Conference of Mayors
Water Environment Federation

cc: Christopher Inglis – EOP/ONCD
Elizabeth Sherwood-Randall – EOP/ONSA/OHSA
Richard Revesz – EOP/OMB/OIRA
Janet McCabe – EPA/AO
Radhika Fox – EPA/OW
Jeffrey Prieto – EPA/OGC
Sean O'Donnell –
EPA/OIG
Tim Del Monico –
EPA/AO/OCIR Victoria Arroyo –
EPA/AO/OP



**Addendum to Joint Association Letter regarding the Pending EO 12866 Regulatory Review: Memorandum to State Drinking Water Administrators on Public Water System Cybersecurity**

**Statutory & Regulatory History**

With increasingly severe cyber threats over the last decade, support has grown at all levels of government and within the sector to enhance water and wastewater system security and resilience. In recent years, the prevailing—and appropriate—trend was a collaborative approach to improving water and wastewater sector-specific cybersecurity through risk and resilience assessments and emergency response planning undertaken by utilities, which Congress has fully endorsed. But within that past eighteen months, EPA has made a significant shift by instead proposing regulation for drinking water utilities through the Sanitary Survey Program, an admittedly "creative"[1] approach, which we find neither practical nor legally supportable. A brief statutory and regulatory history follows:

*America's Water Infrastructure Act of 2018 (AWIA)*

The AWIA (PL 115-270) was passed to improve drinking water and water quality, increase water and wastewater infrastructure investments and jobs, and enhance public health and quality of life. It included significant changes to the Safe Drinking Water Act (SDWA). Among those, AWIA Section 2013 references cybersecurity in addressing community water system risk and resilience. Particularly, this section amended SDWA Section 1433 to require each community water system serving a population of greater than 3,300 persons to conduct a system risk and resilience assessment at least every five years, including the risk from malevolent acts that could "substantially disrupt the ability of the system to provide a safe and reliable supply of drinking

water", which encompasses cyber threats. SDWA § 1433(a). Further, Section 2013 requires such systems to incorporate the findings of their assessment into an emergency response plan, which includes "strategies and resources to improve the resilience of the system, including the physical security and cybersecurity of the system." SDWA § 1433(b). Thus, Congress specifically highlighted cybersecurity as an issue to address through risk and resilience assessments and emergency response planning.

We would also like to call attention to the provision pertaining to alternative preparedness and operational resilience programs. SDWA § 1433(f). Specifically, consistent with section 12(d) of the National Technology Transfer and Advancement Act of 1995, this provision requires EPA to recognize voluntary consensus standards and guidance developed by third-party organizations, like AWWA, that support and facilitate the implementation of the above requirements. For example, AWWA's Cyber Security Assessment Tool and Guidance was developed in collaboration with the National Institute of Standards and Technology (NIST), the Cybersecurity

[1] Statement of Anne Neuberger, Transcript: Securing Cyberspace, The Washington Post (Oct. 13, 2022), https://www.washingtonpost.com/washington-post-live/2022/10/13/transcript-securing-cyberspace/.



and Infrastructure Security Agency (CISA), and EPA representatives in 2014 (and updated in 2019) to provide a consensus-based, sector-specific approach to the NIST cybersecurity framework. Yet, EPA has not leveraged this option to advance the agencies mission in support of AWIA §2013 and related cybersecurity objectives.

*Infrastructure Investment & Jobs Act of 2021*

A significant component of the Infrastructure Investment and Jobs Act (PL 117-58) was greater investment and support to rehabilitate and update water infrastructure, including through several authorizations that support cybersecurity improvements. For example, the Midsize and Large Drinking Water System Infrastructure Resilience and Sustainability Program (sec. 50107) and the Clean Water Infrastructure Resilience and Sustainability Program (sec. 50205) provide grant funding from EPA to help reduce cybersecurity vulnerabilities, among other priorities, at drinking water and wastewater systems. Similarly, the Act (sec. 50113) required EPA and CISA to develop and report to Congress (1) a prioritization framework to identify public drinking water systems that, if degraded or rendered inoperable, would have significant public health and safety impacts, taking into consideration any identified cybersecurity vulnerabilities and independent capacity to address such vulnerabilities, and (2) a technical cybersecurity support plan for public drinking water systems with a methodology for identifying for which systems cybersecurity support should be priorities, timelines for making voluntary technical support available, and specific capabilities that could be utilized to provide such support. These were completed in May 2022[2] and August 2022[3], respectively. Congress did not, however, authorize EPA to develop or otherwise impose cybersecurity requirements on water utilities.

*EPA Unified Agenda – Fall 2021[4]*

In the Fall 2021 Unified Agenda listed EPA/OW RIN 2040-AG20, Cybersecurity in Public Water Systems, as a rulemaking in the final rule stage. EPA indicated that it was evaluating regulatory approaches to improve cybersecurity at public drinking water systems. While EPA planned to offer separate guidance, training, and technical assistance to states and public drinking

water systems on cybersecurity, EPA also announced its plan to issue this Final Interpretive Rule to "provide regulatory clarity and certainty and promote the adoption of cybersecurity measures by public water systems." Particularly, EPA proposed to include cybersecurity assessments as part of the regular drinking water Sanitary Survey Program:

> Sanitary surveys, which states, tribes, or the EPA typically conduct every 3 to 5 years on all public water systems, should include an evaluation of cybersecurity to identify significant deficiencies. EPA recognizes, however, that many states

[2] https://www.epa.gov/system/files/documents/2022-08/Prioritization%20Framework%20RtC%20final.pdf

[3] https://www.epa.gov/system/files/documents/2022-08/9910_RtC-Technical%20Cybersecurity%20Support%20Plan_20220818_final.pdf

[4] https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202110&RIN=2040-AG20



> currently do not assess cybersecurity practices during public water system sanitary surveys. This action is necessary to convey to states that EPA interprets existing regulations for public water system sanitary surveys as including the possible identification of significant deficiencies in cybersecurity practices.

EPA justified the interpretive rule under the Administrative Procedure Act ("APA") as an "interpretation of existing responsibilities under current regulations" stating that "[i]t establishes no new regulatory requirements and, hence, has no regulatory costs or benefits." Importantly, EPA explicitly acknowledged that there were alternatives to the interpretive rule approach, specifically that EPA could "[p]rovide guidance to states, tribes, and EPA on evaluating cybersecurity practices during public water system sanitary surveys without issuing an interpretive rule."

EPA said it would issue a Final Interpretive Rule in April 2022. However, in response to this proposal, in December 2021, water system associations asked EPA to not pursue this regulatory strategy, citing various significant concerns with its legality under the APA, inadequate protection of sensitive information, lack of national consistency given that the Sanitary Survey Program is implemented by states, insufficient skill and training of state staff. (*e.g.*, AWWA 12/9/21 letter, Association of State Drinking Water Administrators 9/29/21, 2/9/22, 11/21/22 letters).

*EPA Unified Agenda – Spring 2022*[5]

Following these public comments, EPA recategorized EPA/OW RIN 2040-AG20, Cybersecurity in Public Water Systems, as a "Long-Term Action" in the Spring 2022 Unified Agenda. Additionally, in a May 2022 budget hearing before the House Committee on Energy and Commerce's Subcommittee on Environment and Climate Change, EPA assured the subcommittee that the Agency would be transparent in its rulemaking processes to allow for proper public notice and comment. Further, when asked about water and wastewater cybersecurity, the Agency indicated that it is "laser focused on this cybersecurity issue" and "using all of our statutory authority to pursue cybersecurity in the water space that we can." Stating further that EPA would not outsource its leadership responsibility in the water and wastewater cybersecurity space, engage regularly with the water sector and the Coordinating Council on Cybersecurity. The Agency committed to making each of these assurances in writing; however, to our knowledge, those written assurances have not been made. The Fiscal Year 2023 EPA Budget, Houston of Representatives,

Subcommittee on Environment and Climate Change, Committee on Energy and Commerce, Washington, D.C. (May 17, 2022) at 1737-1837.

*EPA Unified Agenda – Fall 2022*[6]

The most recent Unified Agenda retitled the "Long Term Action" for EPA/OW RIN 2040-AG20 to "Public Water System Cybersecurity Requirements." This action is summarized

[5] https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202204&RIN=2040-AG20

[6] https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202210&RIN=2040-AG20



as "evaluating regulatory approaches to improve cybersecurity at public water systems. EPA plans to offer separate guidance, training, and technical assistance to states and public water systems on cybersecurity. This action will provide regulatory clarity and promote the adoption of cybersecurity measures by public water systems."

*OMB/OIRA RIN 2040-ZA41 – Memorandum to State Drinking Water Administrators on Public Water System Cybersecurity*

On December 16, 2022, EPA submitted RIN: 2040-ZA41, *Memorandum to State Drinking Water Administrators on Public Water System Cybersecurity*, to OMB/OIRA for review. While EPA has not made the memo or its contents public, we suspect it is substantively the same as the prior proposed interpretive rule. Accordingly, AWWA, AMWA, NRWA, NAWC, WEF, and NACWA requested a meeting with OMB to discuss the memo and express our concerns with a Sanitary Survey Program-based approach.

We are also aware that the Association of State Drinking Water Administrators (ASDWA) had a meeting with OMB expressing similar concerns with the prospective imposition of regulatory burden resulting from this Memo. In addition, concerns were also expressed by AWWA about the Memo and EPA's process during the public comment period of the January 13, 2023, meeting of EPA's Local Government Advisory Committee.

**Response and Recommendations**

While we appreciate that EPA has moved from a Final Interpretive Rule to Long-Term Action, and while the contents of the RIN: 2040-ZA41 memorandum are not yet public, we have significant concerns that EPA has yet to address. Proceeding at this stage with any sort of regulatory requirement would be premature.

First, as explained in a December 9, 2021, letter from AWWA, AMWA, NAWC, and NRWA to Assistant Administrator of Water Radhika Fox: "We do not believe an agency action to establish cybersecurity requirements through an interpretive rule is legally justifiable, as interpretive rules must not set new legal standards or impose new requirements." If the effect of EPA's action is still to impose cybersecurity requirements on operators at public drinking water systems, EPA must satisfy the APA and other legal prerequisites, or may otherwise be subject to judicial review. 5 U.S.C. § 706(2)(A); *Mortg. Bankers Ass'n. v. Harris*, 720 F.3d 966 (D.C. Cir. 2013) (quoting *F.C.C. v. Fox Television Stations*, 556 U.S. 502, 513 (2009) for the holding that

the APA provides the full scope of "judicial authority to review executive agency action for procedural correctness.").

An interpretive rule "simply indicates an agency's reading of a statute or a rule. It does not intend to create new rights or duties, but only reminds affected parties of existing duties." *Paralyzed Veterans of Am. V. West*, 138 F.3d 1434 (Fed. Cir. 1994) (quoting *Orengo Caraballo v. Reich*, 11 F.3d 186, 195 (D.C.Cir.1993)). "The critical feature of interpretive rules is that they are

issued by an agency to advise the public of the agency's construction of the statutes and rules which it administers." *Perez v. Mortgage Bankers Ass'n*, —– U.S. ——–, 135 S.Ct. 1199, 1204, 191 L.Ed.2d 186 (2015) (citation omitted). "The most important factor in differentiating between binding and nonbinding actions is "the actual legal effect (or lack thereof) of the agency action in question. . . Agency action that creates new rights or imposes new obligations on regulated parties or narrowly limits administrative discretion constitutes a legislative rule." *Ass'n of Flight Attendants-CWA, AFL-CIO v. Huerta*, 785 F.3d 710, 717 (D.C. Cir. 2015) (citing *Nat'l Mining Ass'n v. McCarthy*, 758 F.3d 243, 252 (D.C.Cir.2014). The hallmark of an interpretive rule is that such rules are exempt under the APA from public notice and comment requirements. 5 U.S.C. § 553(b)(A). However, when a rule goes beyond that advisory or confirmatory purpose, it is considered a legislative rule, to which public notice and comment requirements apply. 5 U.S.C. § 553(b).

EPA's Memo to add cybersecurity requirements to the Sanitary Survey Program goes well beyond merely providing the "regulatory clarity and certainty" it purports, and does, in fact, establish new regulatory requirements not otherwise imposed under the SDWA. The Sanitary Survey Program is a precondition of state primacy, which is a "systematic program for conducting sanitary surveys of public water systems in the State," which includes an "onsite review of the water source (identifying sources of contamination using results of source water assessments where available), facilities, equipment, operation, maintenance, and monitoring compliance of a public water system to evaluate the adequacy of the system, its sources and operations and the distribution of safe drinking water." SDWA § 1413; 40 C.F.R. §§ 142.10, 142.16. EPA's Memo would seek to add cybersecurity to the state primacy requirements. Although the Sanitary Survey Program requirements generally cover operations, they have never included cybersecurity nor was the Program drafted with cybersecurity in mind — yet EPA is now attempting to tenuously read it in. Such an action would constitute an entirely new requirement, going well beyond the purpose of an interpretive rule. Moreover, SDWA Section 1433 requires that certain drinking water systems conduct risk and resilience assessments that include cybersecurity considerations, then incorporate the assessment findings into an emergency response plan with particulars on how resilience can be improved and implementation of such procedures. It does not, however, require that cybersecurity be part of the state Sanitary Survey Program or be enforced as such. EPA's proposed actions therefore are also inconsistent with Congressional intent.

In addition to this noncompliance with the APA, EPA has not held any open stakeholder engagement on its Final Interpretive Rule or as part of development of the RIN 2040-ZA41 Memorandum, nor has it held a cooperative federalism or Unfunded Mandates Reform Act (2 U.S.C. § 1501 et seq.) consultation with representatives of local and state government. Essentially, EPA has proceeded despite ample opposition from multiple water and wastewater organizations, including state administrators, and without sufficiently engaging with those most affected despite offering assurances to Congressional leaders that such engagements would take place.

More importantly, EPA's proposal to include cybersecurity requirements within the drinking water Sanitary Survey Program administered by state sanitarians is a sub-optimal way to address cybersecurity challenges posed to critical water infrastructure systems. As repeatedly noted by the ASDWA (9/29/21, 2/9/22, 11/21/22 Letters), for example, state authorities that administer the Sanitary Survey Program lack the appropriate staffing, training and expertise to evaluate cybersecurity programs. Even with training, given the complexity of cybersecurity

measures and their relatively rapid evolution, agency staff could misunderstand best practices and their implementation, resulting in an unmerited deficiency or a redirection from a practice that is sufficiently securing the utility. Nothing in federal or state law protects information collected through state agencies' sanitary surveys from being shared publicly, and such disclosures could risk exposing system vulnerabilities to actors who pose cybersecurity threats.

To address these issues and concerns we are committed to working collaboratively with EPA and other stakeholders to develop an effective approach to cybersecurity that is risk- and performance-based. We recognize the necessity to act, and we are committed to working expediently to develop and implement cybersecurity solutions for the water sector that are developed by consensus with critical input and support from water utilities, an approach that is legally sound and will result in a far more effective approach to mitigate cyber threats facing the water sector.

Thus, to best serve our shared goal of cybersecurity solutions for the water sector, we urge you to recall the RIN 2040-ZA41 Memorandum under review at the Office of Management and Budget for reconsideration with stakeholders and to ensure compliance with all applicable laws.

3) Joint Letter to EPA and ICR Regarding Cybersecurity Rule

March 17, 2023

Mr. Michael Regan
Administrator
U.S. Environmental Protection Agency
1200 Pennsylvania Ave, NW
Washington, DC 20460

Mr. Richard Revesz
Administrator
Office of Information and Regulatory Affairs
1650 Pennsylvania Avenue, NW Washington,
DC 20503

**RE: Public Water System Supervision Program (ICR No. 2040-0090)**

Dear Administrator Regan and Administrator Revesz,

The undersigned associations write to you regarding the March 3, 2023 agency action issued by the U.S. Environmental Protection Agency ("EPA") to State Drinking Water Administrators entitled "*Addressing PWS Cybersecurity in Sanitary Surveys or an Alternate Process*" (the "Rule"), which requires states to examine cybersecurity practices and controls at public water systems ("PWS") while conducting sanitary surveys and collect data from PWS regarding the same. This is one of several new substantive requirements imposed by EPA's new final Rule. According to EPA, this Rule is effective immediately. However, the information collection and record keeping requirements associated with this new Rule violate the Paperwork Reduction Act ("PRA") and are not covered by EPA's current Information Collection Request ("ICR") for the Public Water System Supervision Program ("ICR No. 2040-0090"). This ICR covers information collections for "General State Primacy Activities" to implement compliance oversight and enforcement responsibilities under the SDWA. This includes requirements for the primacy agency to maintain records such as the results of sanitary surveys per 40 CFR 142.14. ICR No. 2040-0090 expires on March 31, 2023.[1]

[1] rogram (EPA ICR No. 0270.47), Issued 3/09/2020, https://www.reginfo.gov/public/do/PRAViewICR?ref_nbr=201903-2040-005#

Given the absence of an OMB approved ICR for the information required under the new Rule, state primacy agencies are not authorized to collect this information and public water systems are not required to respond to requests for information.

More specifically, Congress made it very clear in the PRA[2] that an agency shall not conduct or sponsor the collection of information unless in advance of the adoption or revision of the collection of information, the agency has completed all requirements provided in OMB regulations for data collection.[3] This includes publishing a notice in the Federal Register that provides the following:

- a title for the collection of information;
- a summary of the collection of information;
- a brief description of the need for the information and the proposed use of the information;
- a description of the likely respondents and proposed frequency of response to the collection of information;
- an estimate of the burden that shall result from the collection of information;
- notice that comments may be submitted to the agency and OMB; and
- the time period within which the agency is requesting OMB to approve or disapprove the collection of information.

The agency has not fulfilled its obligation to assess burdens the Rule will impose on primacy authorities or PWSs. The Rule requires the collection and review of substantively new and different information than what is currently approved in the current ICR. While the agency's Rule did undergo E.O. 12866 review, no new supporting statement or revised ICR has been prepared or issued for public review and comment.

We are not aware that EPA has given public notice to support renewal of this ICR, that would include providing revised burden estimates, and published a justification of the practical utility of the ICR requirements, especially those contained in the new Rule. Examples of new requirements for primacy agency and PWSs that result in burdens due to the Rule include, but are not limited to, the following:

*Training*[4]

- EPA has released 6 hours of training for states to review the Rule, implementation options and available resources. The training includes a table provided by EPA estimating "*the additional time required for states to assess cybersecurity will be reflective of the population served by the system*."
- EPA has released 6 hours of training for PWSs demonstrating how to use EPA's cybersecurity checklist to assess their program, information on how to address vulnerabilities, and available resources. EPAs checklist includes 33 questions related to various cybersecurity controls for which no estimated time burden is provided, but a majority are classified in the training materials as potential "significant deficiencies" if not implemented.

*Recordkeeping*

- States must maintain records of significant deficiencies and confirmation that the deficiency has been corrected. This requires a modification of existing compliance data systems to add necessary data fields to document cybersecurity related items as part of the sanitary survey.
- States must develop and maintain list of "approved agents" if it allows agents other that the state to conduct the cybersecurity component of the sanitary survey.
- States must add cybersecurity to their annual evaluation of the state's program for conducting sanitary surveys in the report transmitted to EPA.

*Expanded Scope of Coverage*

- EPA records[5] indicate that there are 151,606 PWSs for which this Rule may apply. According to EPA compliance records there are 10,003 community water systems that serve 3,300 or more persons that must comply with AWIA §2013.[6] These systems are mandated by Congress to include an assessment of cybersecurity threats as part of a risk and resilience assessment and an emergency response plan. Therefore, the scope of the Rule captures an additional 141,603 PWSs that would at minimum be required to assess the applicability of the new Rule and associated requirements.

[2] Paperwork Reduction Act, Public Law 104-13, https://www.reginfo.gov/public/reginfo/pra.pdf
[3] 5 CFR 1320 - Controlling Paperwork Burdens on the Public, https://www.govinfo.gov/content/pkg/CFR-2010-title5-vol3/xml/CFR-2010-title5-vol3-part1320.xml
[4] EPA Cybersecurity for the Water Sector – Training, https://www.epa.gov/waterriskassessment/epa-cybersecurity-water-sector#rule

We do not believe that the expiration of the current ICR satisfies any of the criteria that may justify emergency processing by OMB. There is no reasonable explanation for why the agency would be unable to comply with the normal clearance procedures for the existing ICR. The addition of new information collection obligations created by the Rule do not justify emergency processing either since this action has been under consideration by the agency since 2021.[7] Finally, there has been no consultation or collaboration with the organizations

[5] EPA, Safe Drinking Water Information System (SDWIS), 2022Q4 Summary Data

[6] EPA, America's Water Infrastructure Act Section 2013 Compliance Data, https://www.epa.gov/waterresilience/americas-water-infrastructure-act-section-2013-compliance-data

[7] Unified Agenda of Regulatory and Deregulatory Actions, Fall 2021, https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202110&RIN=2040-AG20

representing PWSs regarding considerations that might "minimize the burden" per 5 C.F.R. 1320.13.

Respectfully, we ask that EPA withdraw the Rule until such time that it has fulfilled the statutory obligations defined by the PRA and regulations controlling paperwork burdens on the public. In addition, OMB should provide a statement clarifying that any information collected to support compliance with the Rule would constitute a violation of the PRA and regulations controlling paperwork burdens on the public. We have further concerns with the lack of legally- required procedures followed before issuing the Rule which we look forward to addressing with both the agency and OMB.

Sincerely,

American Water Works Association Association of Metropolitan Water Agencies National Association of Water Companies US Conference of Mayors

cc: Radika Fox – EPA/OW
Tim Del Monico – EPA/OCIR Vicki Arroyo – EPA/OP Jeffrey Prieto – EPA/OGC Sean O'Donnell – EPA/OIG
Jennifer McLain – EPA/OW/OGWDW vers – EPA/OGWDW/WICRD

4) Joint Sanitary Survey Letter to EPA

December 9, 2021

The Honorable Radhika Fox
Assistant Administrator for Water
U.S. Environmental Protection Agency
Washington, DC 20460

Dear Assistant Administrator Fox:

Representatives of the water and wastewater sector have repeatedly raised concerns about the agency's pursuit of issuing a direct final interpretive rule to add cybersecurity to the sanitary survey assessments, but our concerns have not been addressed. Therefore, we feel compelled to express our opposition to the proposed approach.

As you well know, water and wastewater systems are on the front lines of protecting public health and the environment and have exceptional track records doing so. Our members have many years of experience with both sanitary surveys and cybersecurity, and they believe the surveys will be ineffective at improving cybersecurity at water systems.

We believe a solution to securing cybersecurity for the water sector that is arrived at by consensus with and support from water utilities will be far more effective to protect against cyber compromises.

The most effective approach is one that is risk- and performance-based, rather than top-down, one-size-fits-all. This would allow for tailored solutions based each community's unique set of risks, threats, and vulnerabilities.

Among our concerns are:

- We do not believe an agency action to establish cybersecurity requirements through an interpretive rule is legally justifiable, as interpretive rules must not set new legal standards or impose new requirements.

- Nothing in federal or state law protects information collected through sanitary surveys by state agencies from being shared with the public. If, for instance, a state discloses that a utility has a particular vulnerability, the information would be very valuable to hackers looking for an easy target, opening the utility up to ransomware attacks or worse.

- State primacy agency staff are not qualified to assess the cyber readiness of a water system. We anticipate state staff could misunderstand either a best practice or a utility's implementation of said best practice and thus report an unmerited significant deficiency. This could lead to misinformation in the media, reputational harm, and fines. Worse, state primacy agency staff could unintentionally direct a utility toward a practice that is in fact inappropriate for securing the utility and perhaps open the door to a hacker.

- Should a state primacy agency give a utility a clean bill of health and the utility subsequently suffer a compromise, both the state and the utility could be put in legal jeopardy.

- Each state agency may develop their own procedures and recommendations for utilities, leading to a patchwork of regulations across the country. Not only is this burdensome to water utilities that have subdivisions in multiple states, but it will complicate the development of guidance and training by the sector organizations, CISA, and even EPA. Related, many states could go farther than EPA intends in the agency's guidance documents and turn the sanitary survey program into an entirely different regulatory regime.

We are examining various options to effectively protect water systems from cyber threats. We are eager and committed to a collaborative solution that is protective of public health and cyber infrastructure in water utilities, and we would like to work with your office to do so. However, we caution against measures that could fail to have a decisive impact on water sector cybersecurity and that lack input by water sector subject matter experts.

As stewards of public health and the environment, the water sector is ready to accept requirements and accountability that does not do more harm than good or divert resources from water utilities' most effective cybersecurity measures. We look forward to collaborating with you on a better solution that will result in greater cybersecurity in the water sector. We are willing to commit the resources necessary to arrive at one in a reasonable amount of time.

If you would like to discuss our concerns, we would be more than happy to have the conversation.

Sincerely,

G. Tracy Mehan III Diane VanDe Hei
Executive Director, Government Affairs Chief Executive Officer
American Water Works Association Association of Metropolitan Water Agencies

Robert F. Powelson Matthew Holmes
President and Chief Executive Officer Chief Executive Officer
National Association of Water Companies National Rural Water Association

Walter T. Marlowe, P.E.,
CAE Executive Director
Water Environment Federation

cc:
Jennifer McLain/EPA OGWDW David
Travers/EPA WSD
Brian Scott/NSC

5) Letter from APPA

May 16, 2023
The Honorable Morgan Griffith
Chairman, Subcommittee on Oversight & Investigations
House Committee on Energy & Commerce
2125 Rayburn House Office Building
Washington, DC 20515
The Honorable Kathy Castor
Ranking Member, Subcommittee on Oversight & Investigations
House Committee on Energy & Commerce
2322 Rayburn House Office Building
Washington, DC 20515
Dear Chairman Griffith and Ranking Member Castor:
The American Public Power Association (APPA) appreciates the opportunity to submit a statement for
the record for the House Energy & Commerce Committee's Subcommittee on Oversight & Investigation's hearing, "Protecting Critical Infrastructure from Cyberattacks: Examining Expertise of
Sector Specific Agencies."
APPA is the voice of not-for-profit, community-owned utilities that power 2,000 towns and cities
nationwide. APPA represents public power before the federal government to protect the interests of the
more than 49 million people that public power utilities serve, and the 96,000 people they employ. APPA
advocates and advises on electricity policy, technology, trends, training, and operations.
Key Points
• The model of shared responsibility for cybersecurity and resilience, assigning each critical infrastructure sector a Sector-Risk Management Agency (SRMA) to work closely with on a dayto-day basis, while broadly coordinating with the Department of Homeland Security (DHS), has
and continues to be successful; DOE is the energy sector's SRMA.
• The electric sector has strong mandatory and enforceable cyber and physical security standards, including cyber incident reporting, in place.
• Cybersecurity standards and mandates must be risk-based; not all electric utilities have the same
risk profile.
• The federal government should play a greater role in helping electric utilities in assessing vendor
cybersecurity practices, such as establishing a federal vendor certification or accreditation program.
• Congress should pause from consideration of legislation to create additional cyber incident reporting mandates until the Cybersecurity Incident Reporting for Critical Infrastructure Act (CIRCIA) is fully implemented.

• Threats are always evolving, and standards and reporting are only one part of ensuring security.
• Strong industry-government partnerships should be supported to prevent, prepare for, and respond to attacks are vital.


Sector-Risk Management Agencies

In 2013, Presidential Policy Directive 21 – Critical Infrastructure Security and Resilience (PPD-21) established a national policy on critical infrastructure security and resilience. PPD-21 tasked DHS with coordinating the overall federal effort to promote the security and resilience of critical infrastructure.

However, recognizing existing statutory and regulatory authorities of specific departments and agencies, as well as their unique knowledge and specialized expertise, PPD-21 wisely identified 16 critical infrastructure sectors and designated a Sector Risk Management Agency (SRMA) for each sector to "serve as a day-to-day Federal interface for the dynamic prioritization and coordination of sector-specific activities," among other tasks. The Department of Energy (DOE) is the SRMA for the energy sector; within DOE, the Office of Cybersecurity, Energy Security, and Emergency Response (CESER) leads DOE's cybersecurity and energy security mission.

APPA strongly supports the partnership model established in PPD-21, with DOE as the energy sector's SRMA. However, the partnership model is not without complications. This is especially true when it comes to cyber incident reporting. As detailed further below, APPA urges Congress to pause from consideration of legislation to create additional cyber incident reporting mandates on the electric sector until CIRCIA is fully implemented. That would allow for the evaluation of CIRCIA's implementation and a determination of whether further changes are needed.

Mandatory and Enforceable Standards

Congress approved the mandatory and enforceable standards regulatory regime for the bulk power system in the Energy Policy Act of 2005 (EPAct05) (section 215 of the Federal Power Act (FPA)). Under section 215, the North American Electric Reliability Corporation (NERC), working with electric industry experts, regional entities, and government representatives, regularly drafts and updates mandatory reliability standards that apply across the North American grid, including Canada. These standards include the critical infrastructure protection (CIP) standards addressing physical security and cybersecurity.

Participation by industry experts and compliance personnel in the NERC CIP standards development process ensures that the standards are risk-based and technically sound. The Federal Energy Regulatory Commission (FERC) has the power to then approve or remand those standards as they apply in the United States. To ensure compliance, under FERC's oversight, NERC and its regional entities conduct rigorous audits and can levy substantial fines for non-compliance. Additionally, FERC can instruct NERC to develop new or revised reliability standards with a very short turn-around time. CIP standards establish an important baseline of security—but they are a floor, not a ceiling—and grid security is and should be much more than a compliance exercise.

APPA believes that the regulatory regime established in EPAct05 has been very successful due to the deep involvement of technical experts from government and industry alike, as well its iterative nature that allows NERC to identify and respond to developing threats.

Information Sharing and Incident Reporting

The electric sector has long been subject to cyber incident reporting mandates to DOE via an Electricity Emergency Incident and Disturbance Report (OE-417) and through the NERC/FERC process. These requirements are in addition to obligations under individual state laws on data security and data breach reporting that cover many information technology (IT) cyber security incidents. The electric industry has historically had robust voluntary participation in information sharing organizations, including with the Electricity Information Sharing and Analysis Center (E-ISAC) and the Multi-State Information Sharing and Analysis Center for the public power community. Finally, the electric sector has seen increased



adoption of technologies that assist with the visibility and monitoring of its industrial control system and operational technology networks, which also allows some automated sharing of information with the federal government.

Another layer of mandatory cyber incident sharing requirements is expected be added on top of these preexisting requirements through CIRCIA implementation. Signed into law in March 2022, CIRCIA will require covered critical infrastructure entities to report cyber incidents within 72 hours and ransomware

payments within 24 hours to DHS's Cybersecurity and Infrastructure Security Agency (CISA). APPA filed comments in November 2022 in response to a request for information kicking off the CIRCIA rulemaking asking CISA to take a careful and deliberative approach to implementation that accounts for existing reporting mandates and organizations, and to appropriately tailor reporting mandates commensurate with risk to national security.

As outlined above, the electric sector is unique among critical infrastructure sectors in the extent and maturity of existing information sharing regulations and programs. Public power utilities, as units of state and local governments and varying so widely in size and risk profiles, are still more unique. Given these complexities, and pursuant to CIRCIA's explicit intent, it is critical that CISA, DOE, FERC/NERC, and industry are given the time and space necessary to harmonize the new reporting envisioned by CIRCIA with those that already exist. Layering on additional reporting mandates prior to full implementation of CIRCIA would create significant confusion, as well as impose a significant burden on public power utilities with little, if any, security benefits.

Supply Chain Security Challenges

One area of energy sector cybersecurity that would benefit from more involvement from the federal government is supply chain. NERC first adopted supply chain standards in 2017, but a significant challenge for NERC-registered entities in complying with these standards is that vendors are not subject to FERC's jurisdiction under section 215 of the FPA. Supply chain cybersecurity would benefit from a greater federal government role in providing resources that would assist utilities in assessing vendor cybersecurity practices, such as a federal vendor certification or accreditation program. Encouraging domestic manufacturing of necessary products and components would also likely have both supply chain security and reliability benefits. APPA has not yet endorsed a particular approach to vendor accreditation or certification. However, APPA would be concerned with a program structure that places additional requirements on utilities in the expectation that utility vendors would conform to such requirements. Most – if not all – public power utilities would not have the leverage to demand certification from vendors on

their own.1

Public-Private Partnerships

The electric power industry works closely with the federal government, including NERC, FERC, DOE, and DHS, on matters of critical infrastructure protection. One important venue for this collaboration is the Electricity Subsector Coordinating Council (ESCC). The ESCC serves as the principal liaison between the federal government and the electric power sector, with the mission of coordinating efforts to prepare for, and respond to, national-level disasters or threats to critical infrastructure. APPA and public power utilities play a leadership role on the ESCC, which includes utility CEOs and trade association leaders representing all segments of the industry. Their counterparts include senior administration officials from the White House, relevant Cabinet agencies, federal law enforcement, and national security organizations.

APPA works closely with DOE on a number of fronts. Notably, APPA has been awarded three grants since 2016 to help strengthen the cybersecurity posture of public power utilities. Most recently, in September 2022, DOE CESER awarded APPA a grant of $15 million over a three-year period to facilitate the adoption and deployment of industrial control systems cybersecurity technologies for municipal utilities. This builds off an existing $6 million, three-year cooperative agreement (awarded in 2020) to develop and deploy cyber and cyber-physical solutions for public power utilities, and a previous threeyear cooperative agreement (awarded in 2016) to assist small- and medium-sized public power utilities with cyber risk assessment and cybersecurity training. APPA's implementation of these agreements is guided by its Cybersecurity Defense Community working group that includes representatives from public power utilities of varying sizes across the country.

A new program at DOE that is being stood up, the Rural and Municipal Utility Advanced Cybersecurity Grant and Technical Assistance (RMUC), which passed as part of the Infrastructure Investment and Jobs

1 Post-Technical Conference Comments of the American Public Power Association, Joint FERC-DOE Supply Chain Risk Management Technical Conference, December 7, 2022, available at: https://elibrary.ferc.gov/eLibrary/filelist?accession_number=20230217-5199&optimized=false.

Act (P.L. 117-58), is based off the successes of these grant programs. The RMUC is authorized to appropriate a total of $250 million in grants and technical assistance over five years to rural, municipal, and small investor-owned electric utilities to enhance their security posture. APPA appreciates Congress' specific attention to the cybersecurity needs of municipal utilities in this program.

"Defense-in-Depth" and Sector-Wide Preparation Efforts

The goal of every utility and the entire industry is to manage risk prudently. Still, there are tens of thousands of diverse facilities throughout the U.S. and Canada that cannot be protected 100 percent of the time from all threats, requiring utilities to prioritize facilities and assets that, if damaged, would have the most severe impacts on their ability to keep the power on for their community. As such, the electric power industry employs threat mitigation known as "defense-in-depth" that focuses on preparation, prevention, response, and recovery to "all hazard" threats to electric grid operations.

Electric utilities plan and regularly exercise for a variety of emergency situations that could impact their ability to provide electricity. One of the biggest exercises, GridEx, takes place every two years. GridEx VI took place in November 2021 and involved hundreds of organizations and thousands of participants from industry, government agencies, and partners in Canada and Mexico. Managed by NERC and the EISAC, the event included a tabletop exercise where electric sector executives and senior government officials worked through incident response protocols in a scenario involving multiple operating challenges.

The three primary segments of the electric utility industry—public power, investor-owned, and rural electric cooperatives—have long had in place mutual aid response networks to share employees and resources to restore power after natural disasters and other emergencies. The ESCC used the concept of traditional mutual assistance networks to develop the Cyber Mutual Assistance program that can help electric and natural gas companies, public power utilities, and/or rural electric cooperatives restore critical computer systems following significant cyber incidents exceeding an individual entity's capacity to respond. CMA participating entities serve approximately 80 percent of U.S. electric customers and 75 percent of U.S. natural gas customers.

Finally, electric utilities regularly share transformers and other equipment through long existing bilateral and multilateral sharing arrangements and agreements. The industry is expanding equipment sharing programs—like the Spare Transformer Equipment Program (STEP), SpareConnect, and Grid Assurance—to improve grid resiliency.

Conclusion

Public power utilities know that a reliable energy grid is the lifeblood of the nation's economic and national security, as well as vital to the health and safety of all Americans. APPA supports the continued model of shared partnership for cybersecurity and resilience of the energy sector, with DOE as the sector's SRMA. It is critical that Congress and regulators take a risk-based, defense-in-depth approach to promoting cybersecurity of the electric sector, given the diversity of size, model and resources of individual entities. APPA appreciates the opportunity to provide a statement.

Sincerely,

Desmarie Waterhouse

Senior Vice President of Advocacy and Communications & General Counsel