Water 1 - Establish a Water Risk and Resilience Organization

This proposal establishes a North American Energy Reliability Council (NERC)-like entity for the water and wastewater sector to be known as the Water Risk and Resilience Organization (WRRO). The WRRO will be certified by the Environmental Protection Agency (EPA) and will develop cybersecurity risk and resilience requirements for the water sector with oversight from EPA.

A BILL

To establish a Water Risk and Resilience Organization to develop risk and resilience requirements for the water sector.

Sec. X. Water Risk and Resilience Organization

(a) DEFINITIONS.——In this section:

(1) WATER RISK AND RESILIENCE ORGANIZATION.—The terms "Water Risk and Resilience Organization" and "WRRO" means the organization certified by the Environmental Protection Agency (hereafter "Agency") under subsection (c), the purpose of which is to establish and implement risk and resilience requirements for water systems, subject to Agency review.

(2) Cybersecurity RISK AND RESILIENCE REQUIREMENTS.—The term "cybersecurity risk and resilience requirements" means a requirement, approved by the Agency, in consultation with the Cybersecurity and Infrastructure Security Agency and the National Institute of Standards and Technology, under this section, to provide for the reliable operation of a water system. The term describes cybersecurity requirements to support the resilient operation of existing water systems and the cyber resilient design of planned additions or modifications to such systems.

(3) CYBER RESILIENT OPERATION.—The term "cyber resilient operation" means the ability to withstand and reduce the magnitude or duration of disruptive incidents, which includes the capability to anticipate, absorb, adapt to, or rapidly recover from cybersecurity incidents.

(4) CYBERSECURITY INCIDENT.—The term "cybersecurity incident" means a malicious act or suspicious event that disrupts, or attempts to disrupt, the operation of those programmable electronic devices and communication networks including hardware, software and data that are essential to the cyber resilient operation of a water system.

(5) AGENCY.—The term "agency" means the Environmental Protection Agency.

(6) ADMINISTRATOR.—The term "administrator" means the Administrator of the Environmental Protection Agency.

(7) WATER SYSTEM.— The term "water system" means—

(A) A community water system, as defined in 41 U.S.C. §300f(15), that serves a population of 3,300 or more persons.

(B) A treatment works, as defined in 33 U.S.C. §1292(2)(A), that serves a population of 3,300 or more persons.

(b) JURISDICTION AND APPLICABILITY.—

(1) The Administrator shall have jurisdiction, within the United States, over the WRRO certified by the Agency under subsection (c).

(2) The Administrator shall issue a final rule to implement the requirements of this section not later than 270 days after the date of enactment of this section.

(c) CERTIFICATION.—Following the issuance of a rule under subsection (b)(2), any person may submit an application to the Administrator for certification as the WRRO. The Administrator, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency, may certify one such WRRO if the Administrator determines that such WRRO—

(1) demonstrates advanced knowledge and expertise with water sector systems;

(2) is comprised of one or more members with relevant experience as owners and/or operators of water sector systems;

(3) has the ability to develop cybersecurity risk and resilience requirements that provide for an adequate level of cybersecurity risk and resilience of a water system; and

(4) has established rules that—

(A) assure its independence of the users and owners and operators of a water system, while assuring fair stakeholder representation in the selection of its directors and balanced decision making in any WRRO committee or subordinate organizational structure;

(B) allocate equitably reasonable dues, fees, and other charges among end users for all activities under this section;

(C) provide fair and impartial procedures for enforcement of cybersecurity risk and resilience requirements through the imposition of penalties in accordance with subsection (f) (including limitations on activities, functions, or operations, or other appropriate sanctions); and

(D) provide for reasonable notice and opportunity for public comment, due process, openness, and balance of interests in developing cybersecurity risk and resilience requirements and otherwise exercising its duties.

(d) CYBERSECURITY RISK AND RESILIENCE REQUIREMENTS.—

(1) The WRRO shall file each cybersecurity risk and resilience requirement or modification to a requirement that it proposes to be made effective under this section with the Agency.

(2) The Administrator may, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency, approve, by rule or order, a proposed cybersecurity risk and resilience requirement or modification to a requirement if it determines that the requirement is just, reasonable, not unduly discriminatory or preferential, and in the public interest. The Administrator shall defer to the technical expertise of the WRRO with respect to the content of a proposed requirement or modification to a requirement. A proposed requirement or modification shall take effect upon approval by the Administrator.

(3) The Administrator shall remand to the WRRO for further consideration of a proposed

cybersecurity risk and resilience requirement or a modification to a requirement that the Administrator disapproves in whole or in part.

(4) The Administrator, upon his or her own motion or upon complaint, may order the WRRO to submit to the Agency a proposed cybersecurity risk and resilience requirement or a modification to a requirement that addresses a specific matter if the Administrator considers such a new or modified requirement appropriate to carry out this section.

(5) The final rule adopted under subsection (b)(2) shall include specific processes for the identification and timely resolution of any conflict between a cybersecurity risk and resilience requirement and any function, rule, order, tariff, or agreement accepted, approved, or ordered by the Administrator applicable to a water system. A water system shall continue to comply with such function, rule, order, tariff, or agreement accepted, approved, or ordered by the Administrator until—

(A) the Administrator finds a conflict exists between cybersecurity risk and resilience requirement and any such provision;

(B) the Administrator orders a change to such provision; and

(C) the ordered change becomes effective.

(6) If the Administrator determines that a cybersecurity risk and resilience requirement needs to be changed as a result of such a conflict, it shall direct the WRRO to develop and file with the Administrator a modified cybersecurity risk and resilience requirement under paragraph (3) or (4) of this subsection.

(e) WATER SYSTEM MONITORING AND ASSESSMENT.— To aid in the development and adoption of appropriate and necessary cybersecurity risk and resilience requirements and modifications to requirements the WRRO shall—

(1) routinely monitor and conduct periodic assessments of the implementation of cybersecurity risk and resilience requirements, and the effectiveness of cybersecurity risk and resilience requirements for covered water systems in the United States; and

(2) annually submit to the Administrator a report on the implementation of cybersecurity risk and resilience requirements, the effectiveness of cybersecurity risk and resilience requirementsfor covered water systems in the United States, provided that such reports shall only include aggregated or anonymized findings, observations, and data.

(A) The Administrator shall share the contents of a periodic report as required in subparagraph (2) with the Director of the Cybersecurity and Infrastructure Security Agency not later than 30 days following the receipt of a periodic report.

(f) ENFORCEMENT.—

(1) The WRRO may impose, subject to paragraph (2), a penalty on an owner or operator of a water system for a violation of a cybersecurity risk and resilience requirement approved by the Administrator under subsection (d) if the WRRO, after notice and an opportunity for a hearing—

(A) finds that the owner or operator has violated a requirement approved by the Administrator under subsection (d); and

(B) files notice and the record of the proceeding with the Administrator.

(2) The WRRO may not impose a penalty on an owner or operator under paragraph (1) unless the WRRO provides the owner or operator with notice of the alleged violation of a cybersecurity risk and resilience requirement and an opportunity for a consultation and a hearing prior to finding that the owner or operator has violated such requirement under paragraph (1)(A).

(3) A penalty imposed under paragraph (1) may take effect not earlier than the 31st day after the WRRO files with the Administrator notice of the penalty and the record of proceedings.

(4) A penalty imposed under paragraph (1) shall be subject to review by the Administrator, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency, on its own motion or upon application by the water system owner or operator that is the subject of the penalty filed within 30 days after the date such notice is filed with the Administrator. Application to the Administrator for review, or the initiation of review by the Administrator on its own motion, shall not operate as a stay of such penalty unless the Administrator otherwise orders upon its own motion or upon application by the water system owner or operator that is the subject of such penalty. In any proceeding to review a penalty imposed under paragraph (1), the Administrator, after notice and opportunity for hearing (which hearing may consist solely of the record before the WRRO and opportunity for the presentation of supporting reasons to affirm, modify, or set aside the penalty), shall by order affirm, set aside, reinstate, or modify the penalty, and, if appropriate, remand to the WRRO for further proceedings. The Administrator shall implement expedited procedures for such hearings.

(5) On its own motion or upon complaint, the Administrator may order compliance with a cybersecurity risk and resilience requirement and may impose a penalty against a water system owner or operator if the Agency finds, after notice and opportunity for a hearing, that the water system owner or operator has engaged or is about to engage in any acts or practices that constitute or will constitute a violation of a cybersecurity risk and resilience requirement.

(g) SAVINGS PROVISION.—

(1) The WRRO shall have authority to develop cybersecurity risk and resilience requirements for only water systems as defined in subsection (a).

(2) Nothing in this section shall be construed to preempt any authority of any State to take action to ensure the safety, adequacy, and resilience of water service within that State, as long as such action is not inconsistent with any cybersecurity risk and resilience requirement.

(h) STATUS OF WRRO.— The WRRO certified by the Agency under subsection (c) is delegated enforcement authority pursuant to subsection (f) are not departments, agencies, or instrumentalities, of the United States Government.

(i) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to carry out this subsection $5,000,000 for each of fiscal years 2024 and 2025, to remain available until expended by the WRRO.