.....

(Original Signature of Member)

118TH CONGRESS
1ST SESSION

H. R. ||

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

IN THE HOUSE OF REPRESENTATIVES

M@@@@@@@@@@ introduced the following bill; which was referred to the Committee on ■ ■ ■ ■ ■ ■ ■

A BILL

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

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. WATER RISK AND RESILIENCE ORGANIZATION.

(a) DEFINITIONS.—In this section:

(1) ADMINISTRATOR.—The term ''Administrator'' means the Administrator of the Environmental Protection Agency.

(2) AGENCY.—The term ''Agency'' means the Environmental Protection Agency.

(3) COVERED WATER SYSTEM.—The term ''covered water system'' means—

(A) a community water system (as defined in section 1401 of the Safe Drinking Water Act (42 U.S.C. 300f)) that serves a population of 3,300 or more persons; or

(B) a treatment works (as defined in section 212 of the Federal Water Pollution Control Act (33 U.S.C. 1292)) that serves a population of 3,300 or more persons.

(4) CYBER RESILIENT.—The term ''cyber resilient'' means the ability of a covered water or wastewater system to withstand or reduce the magnitude or duration of cybersecurity incidents that disrupt the covered system's ability to function normally and which includes the capability to anticipate, absorb, adapt to, or rapidly recover from cybersecurity incidents.

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

(6) CYBERSECURITY RISK AND RESILIENCE REQUIREMENT.—The term ''cybersecurity risk and resilience requirement'' means a cybersecurity requirement approved by the Administrator under subsection (d) to provide for the cyber resilient operation of a covered water system and the cyber resilient design of planned additions or modifications to such system.

(7) WATER RISK AND RESILIENCE ORGANIZATION.—The terms ''Water Risk and Resilience Organization'' and ''WRRO'' mean the organization certified by the Agency under subsection (c).

(b) JURISDICTION AND APPLICABILITY.—

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

(2) REGULATIONS.—Not later than 270 days after the date of enactment of this Act, the Administrator shall issue a final rule to implement this section to certify the WRRO.

(c) CERTIFICATION.—

(1) IN GENERAL.—Following the issuance of a rule under subsection (b)(2), any person may submit an application to the Administrator for certification as a Water Risk and Resilience Organization.

(2) REQUIREMENTS.—The Administrator shall certify one Water Risk and Resilience Organization if the Administrator determines that such organization—

(A) demonstrates advanced technical knowledge and expertise in the operations of covered water systems;

(B) is comprised of 1 or more members with relevant experience as owners or operators of covered water systems;

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

(D) capable of establishing measures, in line with prevailing best practices, to secure sensitive information and to protect sensitive security information from public disclosure; and

(E) has established rules that require that-

(i) it is independent of the users, owners, and operators of a covered water system, with balanced and objective stakeholder representation in the selection of directors of the organization and balanced decision

making in any committee or subordinate organizational structure;

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

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

(iv) 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 duties.

(d) CYBERSECURITY RISK AND RESILIENCE REQUIREMENTS.—

(1) IN GENERAL.—

(A) PROPOSED REQUIREMENTS.—The WRRO shall propose and file with the Administrator each cybersecurity risk and resilience requirement or modification to a requirement that it proposes to be made effective under this

section.

(B) IMPLEMENTATION PLAN.—For each cybersecurity risk and resilience requirement or modification to such a requirement proposed pursuant to subparagraph (A), the WRRO shall also propose an implementation plan, including the schedule by which covered water systems must achieve compliance with all or parts of the cybersecurity risk and resilience requirement or modification to such a requirement. The enforcement date must provide a reasonable implementation period for covered water systems to meet the requirements under the implementation plan.

(2) APPROVAL.—

(A) IN GENERAL.—Notwithstanding Section (3)(A), the Administrator shall approve, by rule or order, a proposed cybersecurity risk and resilience requirement or modification to such a requirement if the Administrator determines that the requirement is just, reasonable, not unduly discriminatory or preferential.

(B) DEFERENCE TO WRRO.—The Administrator shall defer to the technical expertise of the WRRO with respect to the content of a pro-

posed cybersecurity risk and resilience requirement or modification to such a requirement.

(3) DISAPPROVAL OF REQUIREMENT.—

(A) IN GENERAL.—Notwithstanding Section (2)(A), the Administrator shall remand to the WRRO a proposed cybersecurity risk and resilience requirement or modification to such a requirement for which the Administrator disapproves, in whole or in part, and provide 1 or more specific recommendations that would cause the proposed requirement or modification to be approved under paragraph (2).

(B) RESPONSE AND APPROVAL.—

(i) IN GENERAL.—Upon remand of a proposed cybersecurity risk and resilience requirement or modification to such a requirement and receipt of the Administrator's recommendation pursuant to subparagraph (A), the WRRO shall—

(I) accept the Administrator's recommendation and resubmit an amended proposed cybersecurity risk and resilience requirement or modification to such a requirement consistent with the Administrator's

recommendation;

(II) respond to the Administrator and provide a reason why the recommendation was not accepted; or

(III) withdraw the proposed cybersecurity risk and resilience requirement or modification to such a requirement.

(ii) AMENDED REQUIREMENT.—If the WRRO resubmits a requirement or modification, the Administrator shall review an amended proposed cybersecurity risk and resilience requirement or modification to such requirement submitted by the WRRO pursuant to clause (i)(I) and determine whether to approve such amended requirement in accordance with paragraph (2)(A).

(iii) RESPONSE BY WRRO.—Upon receipt of a response from the WRRO pursuant to clause (i)(II), the Administrator shall—

(I) approve the proposed cybersecurity risk and resilience requirement or modification to such a requirement; or

(II) invite the WRRO to engage in negotiations with the Administrator to reach consensus to address the specific recommendation made by the Administrator under subparagraph (A).

(4) EFFECTIVE DATE.—The effective date of a cybersecurity risk and resilience requirement or modification to such a requirement proposed under this subsection shall be set by the Administrator in accordance with the proposed implementation plan submitted by the WRRO under paragraph (1).

(5) SUBMISSION OF SPECIFIC REQUIREMENT.—The Administrator, upon the Administrator's own motion or upon complaint and having a reasonable basis to conclude existing recommendations under the WRRO are insufficient, when implemented by covered water systems, to protect, defend, mitigate, or recover from a cybersecurity incident, may, following consultation with the WRRO, order the WRRO to submit to the Agency a proposed cybersecurity risk and resilience requirement or a modification to such a requirement that addresses a specific matter if the Administrator considers such a requirement or modified requirement

necessary to protect, defend, mitigate, or recover from a cybersecurity incident.

(6) CONFLICT.—

(A) IN GENERAL.—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 covered water system.

(B) COMPLIANCE.—A water system shall continue to comply with such function, rule, order, tariff, or agreement approved, or otherwise accepted or ordered by the Administrator unless—

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

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

(iii) the ordered change becomes effective.

(C) MODIFICATION.—If the Administrator determines that a cybersecurity risk and resil-

ience requirement needs to be changed as a result of a conflict identified under this paragraph, the Administrator shall direct the WRRO to develop and file with the Administrator a modified cybersecurity risk and resilience requirement under this subsection, undertaken pursuant to the processes in paragraphs 1 through 4 above.

(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, including requiring self-attestations of compliance from covered water systems annually and assessments of the covered water system by the WRRO or a designated third party not less than every five years, 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 requirements for covered water systems in the United States, provided that such reports shall only include aggregated or anonymized findings, observations, and data, and shall not contain any sensitive security information.

(f) ENFORCEMENT.—

(1) IN GENERAL.—The WRRO may impose, subject to paragraphs (2) and (4), a penalty on an owner or operator of a covered 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 of a covered system has violated or failed to comply with a requirement approved by the Administrator under subsection (d); and

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

(2) NOTICE.—The WRRO may not impose a penalty on an owner or operator of a covered system under paragraph (1) unless the WRRO provides the owner or operator with notice of the alleged

violation or failure to comply with 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).

(A) the owner or operator of a covered water system may engage legal Counsel to take part in the consultation and hearing Requirements.

(3) EFFECTIVE DATE OF PENALTY.—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) IMPOSITION OF PENALTY.— A penalty imposed under paragraph (1) shall not exceed $25,000 per day the entity is in violation of a cybersecurity risk and resilience requirement.

(A) A penalty imposed under this subsection shall be the only penalty imposed for the violation. The Administrator is barred from imposing additional penalties on the covered water System for the same violation.

(B) Any penalties collected will be returned to the WRRO to support training initiatives and

support other resource capabilities of the WRRO in carrying out its duties under this Act.

(5) REVIEW BY ADMINISTRATOR.—

(A) IN GENERAL.—A penalty imposed under paragraph (1) may be subject to review by the Administrator.

(B) APPLICATION FOR REVIEW.—The Administrator may conduct a review under subparagraph (A) on the Administrator's own motion or upon application by an owner or operator of a covered water system that is the subject of a penalty imposed under paragraph (1) filed not later than 30 days after notice of such penalty is filed with the Administrator.

(C) STAY OF PENALTY.—A penalty under review by the Administrator under this paragraph may not be stayed unless the Administrator otherwise orders that such penalty be stayed upon the Administrator's own motion or upon application by the owner or operator of the covered water system owner or operator that is the subject of such penalty.

(D) PROCEEDING.—

(i) IN GENERAL.—In any proceeding to review a penalty imposed under para-

graph (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.

(ii) EXPEDITED PROCEDURES.—The Administrator shall act expeditiously in administering all hearings under this section.

(g) SAVINGS PROVISION.—

(1) AUTHORITY.—Nothing in this Act authorizes the WRRO or the EPA Administrator to develop cybersecurity binding risk and resilience requirements for covered water systems, except as defined by this act.

(2) RULE OF CONSTRUCTION.—Nothing in this section may 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

or conflicts with any cybersecurity risk and resilience requirement.

(h) STATUS OF WRRO.—The WRRO certified Under subsection (c) is not a department, agency, or instrumentality 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 to the WRRO until expended.