I

119TH CONGRESS
1ST SESSION

# H. R. 2594

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

---

IN THE HOUSE OF REPRESENTATIVES

APRIL 2, 2025

Mr. CRAWFORD introduced the following bill; which was referred to the Committee on Transportation and Infrastructure, and in addition to the Committee on Energy and Commerce, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

---

# 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) 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.

(3) CYBER RESILIENT.—

(A) IN GENERAL.—The term ''cyber resilient'' means the ability of a covered water system to withstand or reduce the magnitude or duration of cybersecurity incidents that disrupt the ability of the covered water system to function normally.

(B) INCLUSION.—The term ''cyber resilient'' includes the ability of a covered water system 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 programmable electronic devices and communication networks, including hardware,

software, and data that are essential to the cyber resilient operation of a covered water system.

(5) CYBERSECURITY RISK AND RESILIENCE REQUIREMENT.—The term ''cybersecurity risk and resilience requirement'' means a requirement that provides for the cyber resilient operation of a covered water system and the cyber resilient design of planned additions or modifications to a covered water system.

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

(b) APPLICABILITY.—Not later than 270 days after the date of enactment of this Act, the Administrator shall issue a final rule to carry out this section, including regulations for the selection and certification of the WRRO under subsection (c).

(c) CERTIFICATION.—

(1) IN GENERAL.—Following the issuance of the final rule under subsection (b)(1), any organization may submit an application to the Administrator, at such time, in such manner, and containing such information as the Administrator may require,

for certification as the Water Risk and Resilience Organization.

(2) REQUIREMENTS.—The Administrator shall certify not more than 1 organization that submitted an application under paragraph (1) as the Water Risk and Resilience Organization if the Administrator determines that the 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) is 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—

(i) require that the organization be independent of the users, owners, and op-

erators 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) require that the organization 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) provides for reasonable notice and opportunity for public comment, due process, openness, and balancing of interests in developing cybersecurity risk and resilience requirements and otherwise exercising duties described in this section.

(d) CYBERSECURITY RISK AND RESILIENCE REQUIREMENTS.—

(1) IN GENERAL.—

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

(B) IMPLEMENTATION PLAN.—

(i) IN GENERAL.—For each proposed cybersecurity risk and resilience requirement or modification to such a requirement filed pursuant to subparagraph (A), the WRRO shall file an implementation plan, including the schedule for implementation, which may include a specified date, by which covered water systems shall achieve compliance with all of the cybersecurity risk and resilience requirement or modification to such a requirement. The implementation schedule may account for a phased rollout of the requirement, recognizing that the requirement may not apply, in totality, to all covered water systems.

(ii) REASONABLE DEADLINES.—The enforcement date proposed by the WRRO

in the implementation plan under clause (i) shall provide a reasonable implementation period for covered water systems to meet the requirements under the implementation plan.

(2) APPROVAL.—

(A) IN GENERAL.—Notwithstanding paragraph (3)(A), the Administrator shall approve a proposed cybersecurity risk and resilience requirement or modification to such a requirement, including the accompanying implementation plan filed under paragraph (1), if the Administrator determines that the requirement is just, reasonable, and 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 proposed cybersecurity risk and resilience requirement or modification to such a requirement.

(3) DISAPPROVAL OF REQUIREMENT.—

(A) IN GENERAL.—Notwithstanding paragraph (2)(A), if the Administrator disapproves, in whole or in part, a filed cybersecurity risk and resilience requirement or modification to

such a requirement, the Administrator shall remand such requirement to the WRRO and provide to the WRRO specific recommendations that would lead to the approval of the cybersecurity risk and resilience requirement or modification to such requirement under paragraph (2).

(B) TIMELINE.—The Administrator shall remand to the WRRO a proposed cybersecurity risk and resilience requirement or modification to such a requirement disapproved under subparagraph (A), including the submission of the specific recommendations required under that subparagraph, not later than 90 days after the date on which the WRRO filed the requirement or modification with the Administrator under paragraph (1)(A).

(C) RESPONSE AND APPROVAL.—

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

(I) accept the recommendations of the Administrator and resubmit an amended proposed cybersecurity risk and resilience requirement or modification to such a requirement consistent with those recommendations;

(II) provide to the Administrator and 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 files an amended proposed cybersecurity risk and resilience requirement or modification to such a requirement under clause (i)(I) the Administrator shall review such proposed requirement or modification and determine whether to approve such amended requirement or modification in accordance with paragraph (2)(A).

(iii) RESPONSE BY WRRO.—On 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 an approved 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, on the motion of the Administrator or on complaint may, following consultation with the WRRO, order the WRRO to file with the Administrator under paragraph (1) a proposed cybersecurity risk and resilience requirement or modification to such as requirement that addresses a specific matter if the Administrator determines there is a reasonable basis to conclude the existing cyberse-

curity risk and resilience requirements are insufficient, when implemented by covered water systems, to protect, defend, or recover from or mitigate 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 that is applicable to a covered water system.

(B) COMPLIANCE.—A covered water system shall continue to comply with a function, rule, order, tariff, or agreement described in subparagraph (A) unless—

(i) the Administrator finds a conflict exists between a cybersecurity risk and resilience requirement and any function, rule, order, tariff, or agreement approved or otherwise accepted or ordered by the Administrator;

(ii) the Administrator orders a change to that function, rule, order, tariff, or agreement; and

(iii) the ordered change becomes effective.

(C) MODIFICATION.—If the Administrator determines that a cybersecurity risk and resilience requirement needs to be changed as a result of a conflict identified under this paragraph, the Administrator shall direct the WRRO to propose and file with the Administrator a modified cybersecurity risk and resilience requirement pursuant to paragraphs (1) through (4) of this section.

(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 such requirements, the WRRO shall—

(1) routinely monitor and conduct periodic assessments of the implementation of cybersecurity risk and resilience requirements approved by the Administrator under subsection (d) and the effectiveness of cybersecurity risk and resilience requirements for covered systems, including by requiring—

(A) annual self-attestations of compliance with such cybersecurity risk and resilience requirements by covered water systems; and

(B) assessments of the covered water system by the WRRO or by a third party designated by the WRRO not less frequently than every 5 years of compliance by covered water systems with such cybersecurity risk and resilience requirements; and

(2) annually submit to the Administrator a report describing the implementation of cybersecurity risk and resilience requirements approved by the Administrator under subsection (d) and the effectiveness of cybersecurity risk and resilience requirements for covered water systems subject to the requirements that reports under this paragraph—

(A) shall only include aggregated or anonymized findings, observations, and data; and

(B) shall not contain any sensitive security information.

(f) ENFORCEMENT.—

(1) IN GENERAL.—The WRRO may, subject to paragraphs (2) through (5), impose a penalty on the owner or operator of a covered water system for a

violation of a cybersecurity risk and resilience requirement if the WRRO, after notice and an opportunity for a consultation and a hearing—

(A) finds that the owner or operator of a covered system has violated or failed to comply with the cybersecurity risk and resilience requirement; and

(B) files notice of the finding under subparagraph (A) and the record of the proceeding with the Administrator.

(2) NOTICE.—

(A) IN GENERAL.—The WRRO may not impose a penalty on the owner or operator of a covered water system under paragraph (1) unless the WRRO provides the owner or operator with—

(i) notice of the alleged violation of or failure to comply with a cybersecurity risk and resilience requirement; and

(ii) an opportunity for a consultation and a hearing prior to finding that the owner or operator has violated or failed to comply with the applicable cybersecurity risk and resilience requirement under paragraph (1)(A).

(B) ACCESS TO COUNSEL.—The owner or operator of a covered water system may engage legal counsel to take part in the consultation and hearing described in subparagraph (A)(ii).

(3) EFFECTIVE DATE OF PENALTY.—A penalty imposed under paragraph (1) may take effect not earlier than 31 days after the date on which the WRRO files with the Administrator notice of the penalty and the record of proceedings under subparagraph (B) of that paragraph.

(4) IMPOSITION OF PENALTY.—

(A) MAXIMUM AMOUNT.—A penalty imposed under paragraph (1) shall not exceed $25,000 per day the applicable owner or operator is in violation of a cybersecurity risk and resilience requirement approved by the Administrator under subsection (d).

(B) LIMITATION.—No penalty may be imposed on a covered water system under any other provision of law for a violation of a cybersecurity risk and resilience requirement approved by the Administrator under subsection (d).

(C) USE OF PENALTY FUNDS.—Any penalties collected under this subsection shall be re-

turned to the WRRO to support training initiatives and other resource capabilities of the WRRO in carrying out the duties of the WRRO under this section.

(5) REVIEW BY ADMINISTRATOR.—

(A) IN GENERAL.—The Administrator may review a penalty imposed under paragraph (1).

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

(C) STAY OF PENALTY.—A penalty under review by the Administrator under this paragraph may only be stayed if, on the motion of the Administrator or on application by the owner or operator of the covered water system that is the subject of the penalty, the Administrator separately orders the stay of the penalty.

(D) PROCEEDINGS.—

(i) IN GENERAL.—In any proceeding to review a penalty imposed under paragraph (1), the Administrator, after notice and, subject to clause (ii), opportunity for a hearing, shall by order affirm, set aside, reinstate, or modify the penalty, and, if appropriate, remand to the WRRO for further proceedings.

(ii) RECORD BELOW.—A hearing under clause (i) may consist solely of the record before the WRRO and an opportunity for the presentation of supporting reasons to affirm, modify, or set aside the applicable penalty.

(iii) EXPEDITED PROCEDURES.—The Administrator shall act expeditiously in administering all proceedings under this paragraph.

(g) SAVINGS PROVISIONS.—

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

(2) RULE OF CONSTRUCTION.—Nothing in this section preempts 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 in conflict with any cybersecurity risk and resilience requirement.

(h) STATUS OF WRRO.—The WRRO 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 section $10,000,000 to remain available to the WRRO until expended.

○