

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.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. WATER RISK AND RESILIENCE ORGANIZATION.**

4 (a) DEFINITIONS.—In this section:

5 (1) ADMINISTRATOR.—The term “Adminis-
6 trator” means the Administrator of the Environ-
7 mental Protection Agency.

8 (2) COVERED WATER SYSTEM.—The term “cov-
9 ered water system” means—

1 (A) a community water system (as defined
2 in section 1401 of the Safe Drinking Water Act
3 (42 U.S.C. 300f)) that serves a population of
4 3,300 or more persons; or

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

9 (3) CYBER RESILIENT.—

10 (A) IN GENERAL.—The term “cyber resil-
11 ient” means the ability of a covered water sys-
12 tem to withstand or reduce the magnitude or
13 duration of cybersecurity incidents that disrupt
14 the ability of the covered water system to func-
15 tion normally.

16 (B) INCLUSION.—The term “cyber resil-
17 ient” includes the ability of a covered water sys-
18 tem to anticipate, absorb, adapt to, or rapidly
19 recover from cybersecurity incidents.

20 (4) CYBERSECURITY INCIDENT.—The term “cy-
21 bersecurity incident” means a malicious act or sus-
22 picious event that disrupts, or attempts to disrupt,
23 the operation of programmable electronic devices
24 and communication networks, including hardware,

1 software, and data that are essential to the cyber re-
2 silient operation of a covered water system.

3 (5) CYBERSECURITY RISK AND RESILIENCE RE-
4 QUIREMENT.—The term “cybersecurity risk and re-
5 silience requirement” means a requirement that pro-
6 vides for the cyber resilient operation of a covered
7 water system and the cyber resilient design of
8 planned additions or modifications to a covered
9 water system.

10 (6) WATER RISK AND RESILIENCE ORGANIZA-
11 TION; WRRO.—The terms “Water Risk and Resil-
12 ience Organization” and “WRRO” mean the organi-
13 zation certified by the Administrator under sub-
14 section (c).

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

20 (c) CERTIFICATION.—

21 (1) IN GENERAL.—Following the issuance of
22 the final rule under subsection (b)(1), any organiza-
23 tion may submit an application to the Adminis-
24 trator, at such time, in such manner, and containing
25 such information as the Administrator may require,

1 for certification as the Water Risk and Resilience
2 Organization.

3 (2) REQUIREMENTS.—The Administrator shall
4 certify not more than 1 organization that submitted
5 an application under paragraph (1) as the Water
6 Risk and Resilience Organization if the Adminis-
7 trator determines that the organization—

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

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

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

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

23 (E) has established rules that—

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

1 erators of a covered water system, with
2 balanced and objective stakeholder rep-
3 resentation in the selection of directors of
4 the organization and balanced decision
5 making in any committee or subordinate
6 organizational structure;

7 (ii) require that the organization allo-
8 cate reasonable dues, fees, and other
9 charges among end-users for all activities
10 under this section;

11 (iii) provide just and reasonable pro-
12 cedures for enforcement of cybersecurity
13 risk and resilience requirements and the
14 imposition of penalties in accordance with
15 subsection (f), including limitations on ac-
16 tivities, functions, or operations, or other
17 appropriate sanctions; and

18 (iv) provides for reasonable notice and
19 opportunity for public comment, due proc-
20 ess, openness, and balancing of interests in
21 developing cybersecurity risk and resilience
22 requirements and otherwise exercising du-
23 ties described in this section.

24 (d) CYBERSECURITY RISK AND RESILIENCE RE-

25 QUIREMENTS.—

1 (1) IN GENERAL.—

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

8 (B) IMPLEMENTATION PLAN.—

9 (i) IN GENERAL.—For each proposed
10 cybersecurity risk and resilience require-
11 ment or modification to such a require-
12 ment filed pursuant to subparagraph (A),
13 the WRRO shall file an implementation
14 plan, including the schedule for implemen-
15 tation, which may include a specified date,
16 by which covered water systems shall
17 achieve compliance with all of the cyberse-
18 curity risk and resilience requirement or
19 modification to such a requirement. The
20 implementation schedule may account for a
21 phased rollout of the requirement, recog-
22 nizing that the requirement may not apply,
23 in totality, to all covered water systems.

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

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

6 (2) APPROVAL.—

7 (A) IN GENERAL.—Notwithstanding para-
8 graph (3)(A), the Administrator shall approve a
9 proposed cybersecurity risk and resilience re-
10 quirement or modification to such a require-
11 ment, including the accompanying implementa-
12 tion plan filed under paragraph (1), if the Ad-
13 ministrator determines that the requirement is
14 just, reasonable, and not unduly discriminatory
15 or preferential.

16 (B) DEFERENCE TO WRRO.—The Adminis-
17 trator shall defer to the technical expertise of
18 the WRRO with respect to the content of a pro-
19 posed cybersecurity risk and resilience require-
20 ment or modification to such a requirement.

21 (3) DISAPPROVAL OF REQUIREMENT.—

22 (A) IN GENERAL.—Notwithstanding para-
23 graph (2)(A), if the Administrator disapproves,
24 in whole or in part, a filed cybersecurity risk
25 and resilience requirement or modification to

1 such a requirement, the Administrator shall re-
2 mand such requirement to the WRRO and pro-
3 vide to the WRRO specific recommendations
4 that would lead to the approval of the cyberse-
5 curity risk and resilience requirement or modi-
6 fication to such requirement under paragraph
7 (2).

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

18 (C) RESPONSE AND APPROVAL.—

19 (i) IN GENERAL.—On receipt of the
20 remand of a proposed cybersecurity risk
21 and resilience requirement or modification
22 to such a requirement and receipt of the
23 specific recommendations of the Adminis-
24 trator pursuant to subparagraph (A), the
25 WRRO shall—

1 (I) accept the recommendations
2 of the Administrator and resubmit an
3 amended proposed cybersecurity risk
4 and resilience requirement or modi-
5 fication to such a requirement con-
6 sistent with those recommendations;

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

10 (III) withdraw the proposed cy-
11 bersecurity risk and resilience require-
12 ment or modification to such a re-
13 quirement.

14 (ii) AMENDED REQUIREMENT.—If the
15 WRRO files an amended proposed cyberse-
16 curity risk and resilience requirement or
17 modification to such a requirement under
18 clause (i)(I) the Administrator shall review
19 such proposed requirement or modification
20 and determine whether to approve such
21 amended requirement or modification in
22 accordance with paragraph (2)(A).

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

1 (I) approve the proposed cyberse-
2 curity risk and resilience requirement
3 or modification to such a requirement;
4 or

5 (II) invite the WRRO to engage
6 in negotiations with the Administrator
7 to reach consensus to address the spe-
8 cific recommendation made by the Ad-
9 ministrator under subparagraph (A).

10 (4) EFFECTIVE DATE.—The effective date of an
11 approved cybersecurity risk and resilience require-
12 ment or modification to such a requirement pro-
13 posed under this subsection shall be set by the Ad-
14 ministrator in accordance with the proposed imple-
15 mentation plan submitted by the WRRO under para-
16 graph (1).

17 (5) SUBMISSION OF SPECIFIC REQUIREMENT.—
18 The Administrator, on the motion of the Adminis-
19 trator or on complaint may, following consultation
20 with the WRRO, order the WRRO to file with the
21 Administrator under paragraph (1) a proposed cy-
22 bersecurity risk and resilience requirement or modi-
23 fication to such as requirement that addresses a spe-
24 cific matter if the Administrator determines there is
25 a reasonable basis to conclude the existing cyberse-

1 curity risk and resilience requirements are insuffi-
2 cient, when implemented by covered water systems,
3 to protect, defend, or recover from or mitigate a cy-
4 bersecurity incident.

5 (6) CONFLICT.—

6 (A) IN GENERAL.—The final rule adopted
7 under subsection (b)(2) shall include specific
8 processes for the identification and timely reso-
9 lution of any conflict between a cybersecurity
10 risk and resilience requirement and any func-
11 tion, rule, order, tariff, or agreement accepted,
12 approved, or ordered by the Administrator that
13 is applicable to a covered water system.

14 (B) COMPLIANCE.—A covered water sys-
15 tem shall continue to comply with a function,
16 rule, order, tariff, or agreement described in
17 subparagraph (A) unless—

18 (i) the Administrator finds a conflict
19 exists between a cybersecurity risk and re-
20 silience requirement and any function,
21 rule, order, tariff, or agreement approved
22 or otherwise accepted or ordered by the
23 Administrator;

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

4 (iii) the ordered change becomes effective.
5

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

15 (e) WATER SYSTEM MONITORING AND ASSESS-
16 MENT.—To aid in the development and adoption of appropriate
17 and necessary cybersecurity risk and resilience requirements
18 and modifications to such requirements, the
19 WRRO shall—

20 (1) routinely monitor and conduct periodic assessments
21 of the implementation of cybersecurity risk and resilience
22 requirements approved by the Administrator under subsection (d)
23 and the effectiveness of cybersecurity risk and resilience requirements
24 for covered systems, including by requiring—
25

1 (A) annual self-attestations of compliance
2 with such cybersecurity risk and resilience re-
3 quirements by covered water systems; and

4 (B) assessments of the covered water sys-
5 tem by the WRRO or by a third party des-
6 ignated by the WRRO not less frequently than
7 every 5 years of compliance by covered water
8 systems with such cybersecurity risk and resil-
9 ience requirements; and

10 (2) annually submit to the Administrator a re-
11 port describing the implementation of cybersecurity
12 risk and resilience requirements approved by the Ad-
13 ministrator under subsection (d) and the effective-
14 ness of cybersecurity risk and resilience require-
15 ments for covered water systems subject to the re-
16 quirements that reports under this paragraph—

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

20 (B) shall not contain any sensitive security
21 information.

22 (f) ENFORCEMENT.—

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

1 violation of a cybersecurity risk and resilience re-
2 quirement if the WRRO, after notice and an oppor-
3 tunity for a consultation and a hearing—

4 (A) finds that the owner or operator of a
5 covered system has violated or failed to comply
6 with the cybersecurity risk and resilience re-
7 quirement; and

8 (B) files notice of the finding under sub-
9 paragraph (A) and the record of the proceeding
10 with the Administrator.

11 (2) NOTICE.—

12 (A) IN GENERAL.—The WRRO may not
13 impose a penalty on the owner or operator of a
14 covered water system under paragraph (1) un-
15 less the WRRO provides the owner or operator
16 with—

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

20 (ii) an opportunity for a consultation
21 and a hearing prior to finding that the
22 owner or operator has violated or failed to
23 comply with the applicable cybersecurity
24 risk and resilience requirement under para-
25 graph (1)(A).

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

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

11 (4) IMPOSITION OF PENALTY.—

12 (A) MAXIMUM AMOUNT.—A penalty im-
13 posed under paragraph (1) shall not exceed
14 \$25,000 per day the applicable owner or oper-
15 ator is in violation of a cybersecurity risk and
16 resilience requirement approved by the Adminis-
17 trator under subsection (d).

18 (B) LIMITATION.—No penalty may be im-
19 posed on a covered water system under any
20 other provision of law for a violation of a cyber-
21 security risk and resilience requirement ap-
22 proved by the Administrator under subsection
23 (d).

24 (C) USE OF PENALTY FUNDS.—Any pen-
25 alties collected under this subsection shall be re-

1 turned to the WRRO to support training initia-
2 tives and other resource capabilities of the
3 WRRO in carrying out the duties of the WRRO
4 under this section.

5 (5) REVIEW BY ADMINISTRATOR.—

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

8 (B) APPLICATION FOR REVIEW.—The Ad-
9 ministrator may conduct a review under sub-
10 paragraph (A) on the motion of the Adminis-
11 trator or on application by an owner or oper-
12 ator of a covered water system that is the sub-
13 ject of a penalty imposed under paragraph (1),
14 if such application is filed not later than 30
15 days after the date on which the notice of that
16 penalty is filed with the Administrator.

17 (C) STAY OF PENALTY.—A penalty under
18 review by the Administrator under this para-
19 graph may only be stayed if, on the motion of
20 the Administrator or on application by the
21 owner or operator of the covered water system
22 that is the subject of the penalty, the Adminis-
23 trator separately orders the stay of the penalty.

24 (D) PROCEEDINGS.—

1 (i) IN GENERAL.—In any proceeding
2 to review a penalty imposed under para-
3 graph (1), the Administrator, after notice
4 and, subject to clause (ii), opportunity for
5 a hearing, shall by order affirm, set aside,
6 reinstate, or modify the penalty, and, if ap-
7 propriate, remand to the WRRO for fur-
8 ther proceedings.

9 (ii) RECORD BELOW.—A hearing
10 under clause (i) may consist solely of the
11 record before the WRRO and an oppor-
12 tunity for the presentation of supporting
13 reasons to affirm, modify, or set aside the
14 applicable penalty.

15 (iii) EXPEDITED PROCEDURES.—The
16 Administrator shall act expeditiously in ad-
17 ministering all proceedings under this
18 paragraph.

19 (g) SAVINGS PROVISIONS.—

20 (1) AUTHORITY.—Nothing in this section au-
21 thorizes the WRRO or the Administrator to develop
22 binding cybersecurity risk and resilience require-
23 ments for covered water systems, except as specifi-
24 cally provided for in this Act.

1 (2) RULE OF CONSTRUCTION.—Nothing in this
2 section preempts any authority of any State to take
3 action to ensure the safety, adequacy, and resilience
4 of water service within that State, as long as such
5 action is not inconsistent with or in conflict with any
6 cybersecurity risk and resilience requirement.

7 (h) STATUS OF WRRO.—The WRRO is not a depart-
8 ment, agency, or instrumentality of the United States
9 Government.

10 (i) AUTHORIZATION OF APPROPRIATIONS.—There is
11 authorized to be appropriated to carry out this section
12 \$10,000,000 to remain available to the WRRO until ex-
13 pended.

○