

118TH CONGRESS  
2D SESSION

# H. R. 7922

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

---

## IN THE HOUSE OF REPRESENTATIVES

APRIL 10, 2024

Mr. CRAWFORD (for himself and Mr. DUARTE) 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.

1           (2) AGENCY.—The term “Agency” means the  
2 Environmental Protection Agency.

3           (3) COVERED WATER SYSTEM.—The term “cov-  
4 ered water system” means—

5                 (A) a community water system (as defined  
6 in section 1401 of the Safe Drinking Water Act  
7 (42 U.S.C. 300f)) that serves a population of  
8 3,300 or more persons; or

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

13           (4) CYBER RESILIENT.—The term “cyber resil-  
14 ient” means the ability of a covered water or waste-  
15 water system to withstand or reduce the magnitude  
16 or duration of cybersecurity incidents that disrupt  
17 the covered system’s ability to function normally and  
18 which includes the capability to anticipate, absorb,  
19 adapt to, or rapidly recover from cybersecurity inci-  
20 dents.

21           (5) CYBERSECURITY INCIDENT.—The term “cy-  
22 bersecurity incident” means a malicious act or sus-  
23 picious event that disrupts, or attempts to disrupt,  
24 the operation of programmable electronic devices  
25 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 (6) CYBERSECURITY RISK AND RESILIENCE RE-  
4 QUIREMENT.—The term “cybersecurity risk and re-  
5 silience requirement” means a cybersecurity require-  
6 ment approved by the Administrator under sub-  
7 section (d) to provide for the cyber resilient oper-  
8 ation of a covered water system and the cyber resil-  
9 ient design of planned additions or modifications to  
10 such system.

11 (7) WATER RISK AND RESILIENCE ORGANIZA-  
12 TION.—The terms “Water Risk and Resilience Orga-  
13 nization” and “WRRO” mean the organization cer-  
14 tified by the Agency under subsection (c).

15 (b) JURISDICTION AND APPLICABILITY.—

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

19 (2) REGULATIONS.—Not later than 270 days  
20 after the date of enactment of this Act, the Adminis-  
21 trator shall issue a final rule to implement this sec-  
22 tion to certify the WRRO.

23 (c) CERTIFICATION.—

24 (1) IN GENERAL.—Following the issuance of a  
25 rule under subsection (b)(2), any person may submit

1 an application to the Administrator for certification  
2 as a Water Risk and Resilience Organization.

3 (2) REQUIREMENTS.—The Administrator shall  
4 certify one Water Risk and Resilience Organization  
5 if the Administrator determines that such organiza-  
6 tion—

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

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

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

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

22 (E) has established rules that require  
23 that—

24 (i) it is independent of the users, own-  
25 ers, and operators of a covered water sys-

1           tem, with balanced and objective stake-  
2           holder representation in the selection of di-  
3           rectors of the organization and balanced  
4           decision making in any committee or sub-  
5           ordinate organizational structure;

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

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

16          (iv) provide for reasonable notice and  
17          opportunity for public comment, due proc-  
18          ess, openness, and balance of interests in  
19          developing cybersecurity risk and resilience  
20          requirements and otherwise exercising du-  
21          ties.

22          (d) CYBERSECURITY RISK AND RESILIENCE RE-  
23          QUIREMENTS.—

24                  (1) IN GENERAL.—

1           (A) PROPOSED REQUIREMENTS.—The  
2 WRRO shall propose and file with the Adminis-  
3 trator each cybersecurity risk and resilience re-  
4 quirement or modification to a requirement that  
5 it proposes to be made effective under this sec-  
6 tion.

7           (B) IMPLEMENTATION PLAN.—For each  
8 cybersecurity risk and resilience requirement or  
9 modification to such a requirement proposed  
10 pursuant to subparagraph (A), the WRRO shall  
11 also propose an implementation plan, including  
12 the schedule by which covered water systems  
13 must achieve compliance with all or parts of the  
14 cybersecurity risk and resilience requirement or  
15 modification to such a requirement. The en-  
16 forcement date must provide a reasonable im-  
17 plementation period for covered water systems  
18 to meet the requirements under the implemen-  
19 tation plan.

20       (2) APPROVAL.—

21           (A) IN GENERAL.—Notwithstanding para-  
22 graph (3)(A), the Administrator shall approve,  
23 by rule or order, a proposed cybersecurity risk  
24 and resilience requirement or modification to  
25 such a requirement if the Administrator deter-

1 mines that the requirement is just, reasonable,  
2 not unduly Discriminatory, or preferential.

3 (B) DEFERENCE TO WRRO.—The Adminis-  
4 trator shall defer to the technical expertise of  
5 the WRRO with respect to the content of a pro-  
6 posed cybersecurity risk and resilience require-  
7 ment or modification to such a requirement.

8 (3) DISAPPROVAL OF REQUIREMENT.—

9 (A) IN GENERAL.—Notwithstanding para-  
10 graph (2)(A), the Administrator shall remand  
11 to the WRRO a proposed cybersecurity risk and  
12 resilience requirement or modification to such a  
13 requirement for which the Administrator dis-  
14 approves, in whole or in part, and provide 1 or  
15 more specific recommendations that would  
16 cause the proposed requirement or modification  
17 to be approved under paragraph (2).

18 (B) RESPONSE AND APPROVAL.—

19 (i) IN GENERAL.—Upon remand of a  
20 proposed cybersecurity risk and resilience  
21 requirement or modification to such a re-  
22 quirement and receipt of the Administra-  
23 tor’s recommendation pursuant to subpara-  
24 graph (A), the WRRO shall—

1 (I) accept the Administrator’s  
2 recommendation and resubmit an  
3 amended proposed cybersecurity risk  
4 and resilience requirement or modi-  
5 fication to such a requirement con-  
6 sistent with the Administrator’s rec-  
7 ommendation;

8 (II) respond to the Administrator  
9 and provide a reason why the rec-  
10 ommendation was not accepted; or

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

15 (ii) AMENDED REQUIREMENT.—If the  
16 WRRO resubmits a requirement or modi-  
17 fication, the Administrator shall review an  
18 amended proposed cybersecurity risk and  
19 resilience requirement or modification to  
20 such requirement submitted by the WRRO  
21 pursuant to clause (i)(I) and determine  
22 whether to approve such amended require-  
23 ment in accordance with paragraph (2)(A).

24 (iii) RESPONSE BY WRRO.—Upon re-  
25 ceipt of a response from the WRRO pursu-



1 ant to clause (i)(II), the Administrator  
2 shall—

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

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

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

18 (5) SUBMISSION OF SPECIFIC REQUIREMENT.—  
19 The Administrator, upon the Administrator’s own  
20 motion or upon complaint and having a reasonable  
21 basis to conclude existing recommendations under  
22 the WRRO are insufficient, when implemented by  
23 covered water systems, to protect, defend, mitigate,  
24 or recover from a cybersecurity incident, may, fol-  
25 lowing consultation with the WRRO, order the

1 WRRO to submit to the Agency a proposed cyberse-  
2 curity risk and resilience requirement or a modifica-  
3 tion to such a requirement that addresses a specific  
4 matter if the Administrator considers such a re-  
5 quirement or modified requirement necessary to pro-  
6 tect, defend, mitigate, or recover from a cybersecuri-  
7 ty incident.

8 (6) CONFLICT.—

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

17 (B) COMPLIANCE.—A water system shall  
18 continue to comply with such function, rule,  
19 order, tariff, or agreement approved, or other-  
20 wise accepted or ordered by the Administrator  
21 unless—

22 (i) the Administrator finds a conflict  
23 exists between cybersecurity risk and resil-  
24 ience requirement and any such provision;

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

3 (iii) the ordered change becomes effec-  
4 tive.

5 (C) MODIFICATION.—If the Administrator  
6 determines that a cybersecurity risk and resil-  
7 ience requirement needs to be changed as a re-  
8 sult of a conflict identified under this para-  
9 graph, the Administrator shall direct the  
10 WRRO to develop and file with the Adminis-  
11 trator a modified cybersecurity risk and resil-  
12 ience requirement under this subsection, under-  
13 taken pursuant to the processes in paragraphs  
14 (1) through (4) above.

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

20 (1) routinely monitor and conduct periodic as-  
21 sessments, including requiring self-attestations of  
22 compliance from covered water systems annually and  
23 assessments of the covered water system by the  
24 WRRO or a designated third party not less than  
25 every five years, of the implementation of cybersecu-

1 rity risk and resilience requirements, and the effective-  
2 tiveness of cybersecurity risk and resilience require-  
3 ments for covered water systems in the United  
4 States; and

5 (2) annually submit to the Administrator a re-  
6 port on the implementation of cybersecurity risk and  
7 resilience requirements, the effectiveness of cyberse-  
8 curity risk and resilience requirements for covered  
9 water systems in the United States, provided that  
10 such reports shall only include aggregated or  
11 anonymized findings, observations, and data, and  
12 shall not contain any sensitive security information.

13 (f) ENFORCEMENT.—

14 (1) IN GENERAL.—The WRRO may impose,  
15 subject to paragraphs (2) and (4), a penalty on an  
16 owner or operator of a covered water system for a  
17 violation of a cybersecurity risk and resilience re-  
18 quirement approved by the Administrator under sub-  
19 section (d) if the WRRO, after notice and an oppor-  
20 tunity for a hearing—

21 (A) finds that the owner or operator of a  
22 covered system has violated or failed to comply  
23 with a requirement approved by the Adminis-  
24 trator under subsection (d); and

1 (B) files notice and the record of the pro-  
2 ceeding with the Administrator.

3 (2) NOTICE.—The WRRO may not impose a  
4 penalty on an owner or operator of a covered system  
5 under paragraph (1) unless the WRRO provides the  
6 owner or operator with notice of the alleged violation  
7 or failure to comply with a cybersecurity risk and re-  
8 silience requirement and an opportunity for a con-  
9 sultation and a hearing prior to finding that the  
10 owner or operator has violated such requirement  
11 under paragraph (1)(A). The owner or operator of  
12 a covered water system may engage legal Counsel to  
13 take part in the consultation and hearing Require-  
14 ments.

15 (3) EFFECTIVE DATE OF PENALTY.—A penalty  
16 imposed under paragraph (1) may take effect not  
17 earlier than the 31st day after the WRRO files with  
18 the Administrator notice of the penalty and the  
19 record of proceedings.

20 (4) IMPOSITION OF PENALTY.—A penalty im-  
21 posed under paragraph (1) shall not exceed \$25,000  
22 per day the entity is in violation of a cybersecurity  
23 risk and resilience requirement.

24 (A) A penalty imposed under this sub-  
25 section shall be the only penalty imposed for the

1 violation. The Administrator is barred from im-  
2 posing additional penalties on the covered water  
3 System for the same violation.

4 (B) Any penalties collected will be returned  
5 to the WRRO to support training initiatives  
6 and support other resource capabilities of the  
7 WRRO in carrying out its duties under this  
8 Act.

9 (5) REVIEW BY ADMINISTRATOR.—

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

13 (B) APPLICATION FOR REVIEW.—The Ad-  
14 ministrator may conduct a review under sub-  
15 paragraph (A) on the Administrator's own mo-  
16 tion or upon application by an owner or oper-  
17 ator of a covered water system that is the sub-  
18 ject of a penalty imposed under paragraph (1)  
19 filed not later than 30 days after notice of such  
20 penalty is filed with the Administrator.

21 (C) STAY OF PENALTY.—A penalty under  
22 review by the Administrator under this para-  
23 graph may not be stayed unless the Adminis-  
24 trator otherwise orders that such penalty be  
25 stayed upon the Administrator's own motion or

1           upon application by the owner or operator of  
2           the covered water system owner or operator  
3           that is the subject of such penalty.

4           (D) PROCEEDING.—

5           (i) IN GENERAL.—In any proceeding  
6           to review a penalty imposed under para-  
7           graph (1), the Administrator, after notice  
8           and opportunity for hearing (which hearing  
9           may consist solely of the record before the  
10          WRRO and opportunity for the presen-  
11          tation of supporting reasons to affirm,  
12          modify, or set aside the penalty), shall by  
13          order affirm, set aside, reinstate, or modify  
14          the penalty, and, if appropriate, remand to  
15          the WRRO for further proceedings.

16          (ii) EXPEDITED PROCEDURES.—The  
17          Administrator shall act expeditiously in ad-  
18          ministering all hearings under this section.

19          (g) SAVINGS PROVISION.—

20          (1) AUTHORITY.—Nothing in this Act author-  
21          izes the WRRO or the EPA Administrator to de-  
22          velop cybersecurity binding risk and resilience re-  
23          quirements for covered water systems, except as de-  
24          fined by this act.

1           (2) RULE OF CONSTRUCTION.—Nothing in this  
2 section may be construed to preempt any authority  
3 of any State to take action to ensure the safety, ade-  
4 quacy, and resilience of water service within that  
5 State, as long as such action is not inconsistent with  
6 or conflicts with any cybersecurity risk and resilience  
7 requirement.

8           (h) STATUS OF WRRO.—The WRRO certified under  
9 subsection (c) is not a department, agency, or instrumen-  
10 tality of the United States Government.

11          (i) AUTHORIZATION OF APPROPRIATIONS.—There is  
12 authorized to be appropriated to carry out this subsection  
13 \$5,000,000 for each of fiscal years 2024 and 2025, to re-  
14 main available to the WRRO until expended.

○