

119TH CONGRESS
2D SESSION

S. 5368

To amend the Safe Drinking Water Act and the Federal Water Pollution Control Act to establish or modify cybersecurity requirements for drinking water and wastewater systems, and for other purposes.

IN THE SENATE OF THE UNITED STATES

AUGUST 7, 2026

Mr. SCHIFF (for himself and Ms. KLOBUCHAR) introduced the following bill; which was read twice and referred to the Committee on Environment and Public Works

A BILL

To amend the Safe Drinking Water Act and the Federal Water Pollution Control Act to establish or modify cybersecurity requirements for drinking water and wastewater systems, and for other purposes.

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. SHORT TITLE; TABLE OF CONTENTS.**

4 (a) SHORT TITLE.—This Act may be cited as the
5 “Water Cyber Shield Act of 2026”.

6 (b) TABLE OF CONTENTS.—The table of contents for
7 this Act is as follows:

Sec. 1. Short title; table of contents.

TITLE I—DRINKING WATER INFRASTRUCTURE

- Sec. 101. Community water system risk and resilience.
 Sec. 102. Cybersecurity requirements for drinking water systems.
 Sec. 103. Reauthorization of midsize and large drinking water system infrastructure resilience and sustainability program.
 Sec. 104. Drinking water security assistance.

TITLE II—CLEAN WATER INFRASTRUCTURE

- Sec. 201. Treatment works risk and resilience.
 Sec. 202. Cybersecurity requirements for treatment works.
 Sec. 203. Reauthorization of the clean water infrastructure resiliency and sustainability program.
 Sec. 204. Clean water security assistance.

TITLE III—CYBER INCIDENT REPORTING OBLIGATIONS

- Sec. 301. Cyber incident reporting.

1 **TITLE I—DRINKING WATER**
 2 **INFRASTRUCTURE**
 3 **SEC. 101. COMMUNITY WATER SYSTEM RISK AND RESIL-**
 4 **IENCE.**

5 Section 1433 of the Safe Drinking Water Act (42
 6 U.S.C. 300i–2) is amended—

7 (1) in subsection (a)—

8 (A) in paragraph (1)(A)—

9 (i) in clause (ii), by striking “storage
 10 and distribution facilities, electronic, com-
 11 puter, or other automated systems (includ-
 12 ing the security of such systems) which”
 13 and inserting “and storage and distribu-
 14 tion facilities that”;

15 (ii) in clause (v), by striking “and” at
 16 the end; and

1 (iii) by adding at the end the fol-
 2 lowing:

3 “(vii) using a method approved by the
 4 applicable State, the risks to electronic,
 5 computer, or other automated systems for
 6 the purpose of identifying significant cy-
 7 bersecurity risks that have the potential to
 8 cause the impacts described in subpara-
 9 graph (A) or (B) of paragraph (2); and”;
 10 and

11 (B) by striking paragraphs (3) through (5)
 12 and inserting the following:

13 “(3) REVIEW AND REVISION.—

14 “(A) IN GENERAL.—Each community
 15 water system described in paragraph (1) shall,
 16 not less frequently than once every 5 years, re-
 17 view and, if necessary, revise the assessment.

18 “(B) CERTIFICATION TO THE ADMINIS-
 19 TRATOR OR STATE.—On completion of the re-
 20 view under subparagraph (A), a community
 21 water system described in paragraph (1) shall
 22 submit to the applicable State a certification
 23 that the community water system has reviewed
 24 and, if applicable, revised the assessment.”;

25 (2) in subsection (b)—

1 (A) by redesignating paragraphs (1)
 2 through (4) as subparagraphs (A) through (D),
 3 and indenting appropriately;

4 (B) in the matter preceding subparagraph
 5 (A) (as so redesignated), by striking “Each
 6 community water system” in the first sentence
 7 and all that follows through “The emergency
 8 response plan” in the third sentence and insert-
 9 ing the following:

10 “(1) IN GENERAL.—Each community water sys-
 11 tem serving a population greater than 3,300 shall
 12 prepare an emergency response plan that incor-
 13 porates findings of the assessment conducted under
 14 subsection (a) for that community water system (or
 15 any revisions to that assessment).

16 “(2) REQUIRED INCLUSIONS.—The emergency
 17 response plan of a community water system under
 18 paragraph (1)”;

19 (C) in paragraph (2) (as so designated)—

20 (i) in subparagraph (A) (as so redes-
 21 ignated), by striking “and cybersecurity”;

22 (ii) in subparagraph (C) (as so redes-
 23 ignated), by striking “and” at the end;

1 (iii) in subparagraph (D) (as so redes-
 2 ignated), by striking the period at the end
 3 and inserting “; and”; and

4 (iv) by adding at the end the fol-
 5 lowing:

6 “(E) countermeasures that the system in-
 7 tends to adopt or, if already in use, maintain to
 8 mitigate the significant cybersecurity risks iden-
 9 tified under subsection (a)(1)(A)(vii), including
 10 a schedule the system intends to follow to adopt
 11 any countermeasures not already in use by the
 12 system.”; and

13 (D) by adding at the end the following:

14 “(3) REVIEW; REVISION.—A community water
 15 system serving a population greater than 3,300 shall
 16 review and, as necessary, revise the emergency re-
 17 sponse plan prepared under this subsection not less
 18 frequently than once every 5 years.”;

19 (3) by striking subsection (f);

20 (4) by redesignating subsections (c), (d), and
 21 (e) as subsections (d), (e), and (f), respectively;

22 (5) by inserting after subsection (b) the fol-
 23 lowing:

24 “(c) SUBMISSION AND APPROVAL OF ASSESSMENTS
 25 AND PLANS.—

1 “(1) SUBMISSION.—

2 “(A) IN GENERAL.—Each community
3 water system subject to subsections (a) and (b)
4 shall, during a cybersecurity assessment pursu-
5 ant to section 1433A(b)(1)(A), provide to the
6 applicable State—

7 “(i) the portion of the assessment pre-
8 pared under subsection (a) that is de-
9 scribed in paragraph (1)(A)(vii) of that
10 subsection (including any revision to that
11 portion of the assessment); and

12 “(ii) the portion of the emergency re-
13 sponse plan prepared under subsection (b)
14 that is described in paragraph (2)(E) of
15 that subsection (including any revision to
16 that portion of the emergency response
17 plan).

18 “(B) LIMITATION.—Neither the Adminis-
19 trator nor a State may require the submission
20 of any portion of an assessment under sub-
21 section (a) or an emergency response plan
22 under subsection (b) that is not described in
23 subparagraph (A).

24 “(2) REVIEW; APPROVAL.—

25 “(A) IN GENERAL.—A State shall—

1 “(i) review the portions of the assess-
2 ments and emergency response plans of
3 community water systems submitted pur-
4 suant to paragraph (1)(A) for conformity
5 with the requirements of this section and
6 section 1433A; and

7 “(ii)(I) approve of the portions of an
8 assessment and emergency response plan
9 submitted pursuant to paragraph (1)(A);
10 or

11 “(II) disapprove of the portions of an
12 assessment and emergency response plan
13 submitted pursuant to paragraph (1)(A) if
14 the Administrator or State, as applicable,
15 determines that—

16 “(aa) the submitted portions of
17 the assessment or emergency response
18 plan are missing, incomplete, or fail to
19 conform with the requirements of this
20 section or section 1433A; or

21 “(bb) the submitted portions of
22 the assessment or emergency response
23 plan fail to provide for cybersecurity
24 resilience in accordance with the base-
25 line cybersecurity standards estab-

1 lished by the Administrator under sec-
2 tion 1433A(c).

3 “(B) ENFORCEMENT.—A State may use
4 appropriate enforcement mechanisms under this
5 title or the appropriate State authority to rem-
6 edy noncompliance, as described in items (aa)
7 and (bb) of subparagraph (A)(ii)(II), under this
8 subsection.

9 “(3) SUBMITTED DOCUMENTATION.—

10 “(A) APPLICABILITY OF FOIA.—Any infor-
11 mation submitted under this subsection shall be
12 exempt from disclosure under section 552(b)(3)
13 of title 5, United States Code (commonly known
14 as the ‘Freedom of Information Act’), and any
15 provision of State, Tribal, or local freedom of
16 information law, open government law, open
17 meetings law, open records law, sunshine law,
18 or similar law requiring disclosure of informa-
19 tion or records.

20 “(B) TREATMENT OF DOCUMENTATION.—

21 “(i) PROTOCOL DEVELOPMENT.—Not
22 later than 180 days after the date of en-
23 actment of the Water Cyber Shield Act of
24 2026 and before any cybersecurity assess-
25 ments are carried out pursuant to section

1 1433A(b)(1)(A), the Administrator, in con-
2 sultation with appropriate Federal law en-
3 forcement and intelligence officials, shall
4 develop such protocols as are necessary to
5 protect any information provided under
6 paragraph (1)(A) to the State.

7 “(ii) REQUIREMENTS FOR PRO-
8 TOCOL.—The protocol developed under
9 clause (i) shall ensure that—

10 “(I) each copy of the portions of
11 an assessment and emergency re-
12 sponse plan submitted pursuant to
13 paragraph (1)(A) are kept in a secure
14 location;

15 “(II) only individuals designated
16 by the applicable State may have ac-
17 cess to copies of the portions of the
18 assessment and emergency response
19 plan submitted pursuant to paragraph
20 (1)(A); and

21 “(III) no copy of the portions of
22 the assessment and emergency re-
23 sponse plan submitted pursuant to
24 paragraph (1)(A) shall be made avail-
25 able to anyone other than an indi-

1 vidual designated by the applicable
2 State.

3 “(iii) SAVINGS PROVISION.—Nothing
4 in this subparagraph authorizes any person
5 to withhold any information from Congress
6 or from a committee or subcommittee of
7 Congress.”;

8 (6) in subsection (e) (as so redesignated), by
9 striking “a certification of such assessment or plan
10 is submitted to the Administrator” and inserting
11 “an assessment or plan is submitted to the applica-
12 ble State,”; and

13 (7) by striking subsection (h) and inserting the
14 following:

15 “(h) DEFINITIONS.—In this section:

16 “(1) NATURAL HAZARD.—The term ‘natural
17 hazard’ means a natural event that threatens the
18 functioning of a community water system, including
19 an earthquake, tornado, flood, hurricane, wildfire,
20 and hydrologic changes.

21 “(2) RESILIENCE.—The term ‘resilience’ means
22 the ability of a community water system or an asset
23 of a community water system to adapt to or with-
24 stand the effects of a malevolent act or natural haz-
25 ard without interruption to the asset’s or system’s

function, or if the function is interrupted, to rapidly return to a normal operating condition.

“(3) STATE.—

“(A) IN GENERAL.—The term ‘State’ means a State that has assumed primary enforcement responsibility pursuant to section 1433A(e).

“(B) ENFORCEMENT BY THE ADMINISTRATOR.—If a State has not assumed primary enforcement responsibility pursuant to section 1433A(e), the term ‘State’ shall, for purposes of obligations of the State under this subsection, be considered to be a reference to the Administrator.”.

SEC. 102. CYBERSECURITY REQUIREMENTS FOR DRINKING WATER SYSTEMS.

(a) IN GENERAL.—The Safe Drinking Water Act is amended by inserting after section 1433 (42 U.S.C. 300i–2) the following:

“SEC. 1433A. CYBERSECURITY REQUIREMENTS.

“(a) DEFINITIONS.—In this section:

“(1) CYBERSECURITY INCIDENT.—The term ‘cybersecurity incident’ means a malicious act or suspicious event that disrupts, or attempts to disrupt, the operation of programmable electronic de-

1 vices and communication networks, including hard-
2 ware, software, and data that are essential to the cy-
3 bersecurity resilience of a public water system.

4 “(2) CYBERSECURITY RESILIENCE.—The term
5 ‘cybersecurity resilience’ means the ability of a pub-
6 lic water system to adapt to or withstand the effects
7 of a cybersecurity incident without interruption to
8 the public water system’s function, or if the function
9 is interrupted, to rapidly return to a normal oper-
10 ating condition.

11 “(3) STATE.—

12 “(A) IN GENERAL.—Except for subsection
13 (e), the term ‘State’ means a State that has as-
14 sumed primary enforcement responsibility pur-
15 suant to subsection (e).

16 “(B) ENFORCEMENT BY THE ADMINIS-
17 TRATOR.—If a State has not assumed primary
18 enforcement responsibility pursuant to sub-
19 section (e), the term ‘State’ shall, for purposes
20 of obligations of the State under this section
21 (except for subsection (e)), be considered to be
22 a reference to the Administrator.

23 “(b) CYBERSECURITY ASSESSMENTS.—

24 “(1) ASSESSMENTS REQUIRED.—

1 “(A) IN GENERAL.—A State shall carry
2 out cybersecurity assessments of public water
3 systems in accordance with this paragraph.

4 “(B) EVALUATION OF ADEQUACY.—For a
5 public water system subject to a cybersecurity
6 assessment under subparagraph (A), if the pub-
7 lic water system uses operational technology,
8 the State shall evaluate the adequacy of the cy-
9 bersecurity of the operational technology, and
10 information and communications technology
11 that is connected to the operational technology,
12 against the baseline cybersecurity standards
13 promulgated by the Administrator under sub-
14 section (c).

15 “(C) REVIEW OF ASSESSMENTS AND
16 PLANS.—In carrying out a cybersecurity assess-
17 ment required under subparagraph (A), a pub-
18 lic water system shall provide, and the State
19 shall review, the portions of the risk and resil-
20 ience assessments of the public water system
21 under section 1433(a) and the emergency re-
22 sponse plans of the public water system under
23 section 1433(b) submitted under section
24 1433(c)(1)(A).

1 “(D) INSPECTIONS.—In carrying out cy-
2 bersecurity assessments under this paragraph, a
3 State shall carry out inspections of a represent-
4 ative sample of public water systems each year,
5 which sampling shall be informed by risk-based
6 considerations, subject to the condition that the
7 scope of the inspection is limited to the systems
8 of the public water system necessary to meet
9 the requirements of this paragraph.

10 “(2) VIOLATIONS.—If a State identifies a viola-
11 tion of the baseline cybersecurity standards estab-
12 lished by the Administrator under subsection (c)
13 while conducting an assessment under paragraph
14 (1), the State shall take appropriate steps to ensure
15 that the public water system addresses the violation
16 and use mechanisms, including enforcement, for fail-
17 ures to correct those violations.

18 “(3) SUBMISSION TO EPA.—

19 “(A) IN GENERAL.—A State shall annually
20 submit to the Administrator a report that sum-
21 marizes the performance of the public water
22 systems of the State for each cybersecurity per-
23 formance metric established by the Adminis-
24 trator under subsection (d)(1) based on the re-

1 view by the State of risk and resilience assess-
2 ments pursuant to paragraph (1)(C).

3 “(B) REQUIREMENT.—A report submitted
4 under subparagraph (A) shall not identify any
5 specific public water system and shall include
6 only aggregations of data.

7 “(4) TECHNICAL ASSISTANCE.—The Adminis-
8 trator shall, on request of a public water system,
9 provide guidance and technical assistance to the
10 public water system with respect to—

11 “(A) implementing any requirement under
12 this section or section 1433; and

13 “(B) enhancing cybersecurity resilience.

14 “(c) BASELINE CYBERSECURITY STANDARDS.—

15 “(1) IN GENERAL.—The Administrator shall by
16 rulemaking establish baseline cybersecurity stand-
17 ards that shall serve as requirements to provide for
18 the cybersecurity resilience of a public water system.

19 “(2) REQUIREMENTS.—In developing and es-
20 tablishing the baseline cybersecurity standards under
21 paragraph (1), the Administrator shall, at a min-
22 imum—

23 “(A) work in conjunction with the Director
24 of the Cybersecurity and Infrastructure Secu-

1 rity Agency and the Director of the National
2 Institute of Standards and Technology;

3 “(B) develop the baseline cybersecurity
4 standards in collaboration with public water
5 systems of various sizes and capacities to en-
6 sure that feedback from a variety of public
7 water systems is considered during the develop-
8 ment of the baseline cybersecurity standards;

9 “(C) ensure that best practices and guide-
10 lines that already exist in the water sector at
11 the time of the development of the baseline cy-
12 bersecurity standards inform the development
13 of the baseline cybersecurity standards;

14 “(D) establish a technical advisory com-
15 mittee to provide input with respect to, review,
16 and refine the baseline cybersecurity standards
17 throughout the development process, which
18 shall, at a minimum, include—

19 “(i) representatives from public water
20 systems of various sizes;

21 “(ii) professional water associations;

22 “(iii) cybersecurity experts;

23 “(iv) a representative from a relevant
24 voluntary consensus standards body, as de-
25 scribed in section 12(d)(1) of the National

Technology Transfer and Advancement Act
of 1995 (15 U.S.C. 272 note; Public Law
104–113); and

“(v) a representative from an infor-
mation technology or operational tech-
nology service provider that provides cyber-
security services to public water systems;
and

“(E) consult with the States.

“(3) CONSIDERATION OF VARIED CAPACITY
AND RISK.—In developing the baseline cybersecurity
standards under paragraph (1), the Administrator—

“(A) shall ensure that the baseline cyberse-
curity standards account for the varied capacity
and risk of all public water systems; and

“(B) may establish different baseline cy-
bersecurity standards for different categories of
public water systems subject to assessments
under subsection (b) based on capacity or risk.

“(d) CYBERSECURITY PERFORMANCE METRICS.—

“(1) ESTABLISHMENT OF METRICS.—

“(A) IN GENERAL.—Not later than 2 years
after the date of enactment of this section, the
Administrator shall establish cybersecurity per-
formance metrics (referred to in this subsection

1 as the ‘cybersecurity performance metrics’) to
2 be used by the Administrator to measure or as-
3 sess how well the sector of public water systems
4 in the United States is making progress on im-
5 plementing cybersecurity best practices.

6 “(B) ASSESSMENT; REPORT.—The Admin-
7 istrator shall, not less frequently than once
8 every 4 years—

9 “(i) assess the sector of public water
10 systems in the United States using the cy-
11 bersecurity performance metrics; and

12 “(ii) submit to Congress and make
13 publicly available a report describing, on a
14 generalized, sector-wide basis, the state of
15 public water systems sector performance
16 using the assessment carried out under
17 clause (i).

18 “(2) PROVISION OF INFORMATION.—Notwith-
19 standing any other provision of law, a public water
20 system may, at the discretion of the public water
21 system and for the purpose of developing sector-wide
22 risk assessments and performance metrics to meas-
23 ure how public water systems are making progress
24 in developing and implementing cybersecurity best
25 practices, provide to the Administrator, and the Ad-

1 administrator may accept, information that would as-
 2 sist the Administrator in the development and main-
 3 tenance of cybersecurity performance metrics.

4 “(e) ENFORCEMENT; STATE ASSUMPTION OF DU-
 5 TIES.—

6 “(1) IN GENERAL.—This section and section
 7 1433 shall be enforced by the Administrator unless
 8 a State assumes primary enforcement responsibility
 9 pursuant to this subsection.

10 “(2) APPLICATION.—A State seeking to assume
 11 primary enforcement responsibility pursuant to this
 12 subsection shall submit to the Administrator an ap-
 13 plication at such time, in such manner, and con-
 14 taining such information as the Administrator may
 15 by regulation require.

16 “(3) DETERMINATION.—On receiving an appli-
 17 cation described in paragraph (2) from a State, the
 18 Administrator shall, based on that application, de-
 19 termine whether the State—

20 “(A) has adopted and is implementing ade-
 21 quate procedures for the enforcement of re-
 22 quirements that are no less stringent than those
 23 under this section and section 1433;

1 “(B) has adopted authority and has suffi-
2 cient capacity to impose enforcement remedies
3 in line with those prescribed under this title;

4 “(C) has sufficient capacity and personnel
5 with sufficient expertise to perform cybersecu-
6 rity assessments and conduct reviews of risk
7 and resilience assessments and emergency re-
8 sponse plans under section 1433; and

9 “(D) has sufficient security mechanisms in
10 place to prevent any unsanctioned disclosure or
11 dissemination of risk and resilience assess-
12 ments, emergency response plans, and any
13 other information provided by a public water
14 system, in alignment with the protocols devel-
15 oped by the Administrator under section
16 1433(c)(3)(B)(i).

17 “(4) TIMELINE.—Not later than 180 days after
18 the date on which the Administrator receives an ap-
19 plication described in paragraph (2), the Adminis-
20 trator shall—

21 “(A) if the Administrator determines that
22 the State meets each requirement described in
23 paragraph (3), grant the application; or

24 “(B) if the Administrator determines that
25 the State fails to meet 1 or more of the require-

1 ments described in paragraph (3), deny the ap-
2 plication.

3 “(5) REVOCATION OF PRIMARY ENFORCEMENT
4 RESPONSIBILITY.—The Administrator may, as ap-
5 propriate, revoke an assumption of primary enforce-
6 ment responsibility pursuant to this subsection if the
7 Administrator determines that a State no longer
8 meets 1 or more requirements described in para-
9 graph (3).

10 “(6) REGULATIONS REQUIRED.—The Adminis-
11 trator shall promulgate regulations carrying out this
12 subsection not later than 1 year after the date of en-
13 actment of this section, which shall include—

14 “(A) the requirements for an application
15 described in paragraph (2);

16 “(B) the period for which a State may as-
17 sume primary enforcement responsibility pursu-
18 ant to this subsection before renewal; and

19 “(C) the manner by which the Adminis-
20 trator may revoke primary enforcement respon-
21 sibility pursuant to paragraph (5).

22 “(7) SAVINGS PROVISION.—An assumption of
23 primary enforcement responsibility pursuant to this
24 subsection shall be separate from any authority as-
25 sumed under section 1413.”.

1 (b) ENFORCEMENT AUTHORITY.—Section 1414(i)(1)
 2 of the Safe Drinking Water Act (42 U.S.C. 300g–3(i)(1))
 3 is amended by inserting “1433A,” after “1433,”.

4 (c) RECORDS AND INSPECTIONS.—Section
 5 1445(b)(1) of the Safe Drinking Water Act (42 U.S.C.
 6 300j–4(b)(1)) is amended, in the first sentence—

7 (1) by striking “or (C) any” and inserting “(C)
 8 any”;

9 (2) by inserting “or (D) a requirement to un-
 10 dergo an inspection under section 1433A(a)(2)(D),”
 11 after “subsection (a),”; and

12 (3) by striking “or (C), is” and inserting “(C),
 13 or (D), is”.

14 (d) CONFORMING AMENDMENT.—Section 1413(a) of
 15 the Safe Drinking Water Act (42 U.S.C. 300g–2(a)) is
 16 amended, in the matter preceding paragraph (1), by in-
 17 serting “(except for sections 1433 and 1433A)” after
 18 “this title”.

19 **SEC. 103. DRINKING WATER SECURITY ASSISTANCE.**

20 (a) AUTHORIZATION OF APPROPRIATIONS.—In addi-
 21 tion to any amounts authorized to be appropriated under
 22 section 1452(m) of the Safe Drinking Water Act (42
 23 U.S.C. 300j–12(m)), there is authorized to be appro-
 24 priated \$300,000,000 for each of fiscal years 2027
 25 through 2032 for the purposes of helping public water sys-

1 tems (as defined in section 1401 of that Act (42 U.S.C.
2 300f)) build cybersecurity resilience (as defined in section
3 1433A(a)(1) of the Safe Drinking Water Act) and identi-
4 fying and mitigating cybersecurity vulnerabilities, includ-
5 ing those included in risk and resilience assessments and
6 emergency response plans prepared pursuant to section
7 1433 of that Act (42 U.S.C. 300i–2).

8 (b) GUIDANCE.—The Administrator of the Environ-
9 mental Protection Agency may issue guidance to deter-
10 mine specific criteria for eligible uses of the amounts made
11 available under subsection (a) that further the purposes
12 described in that subsection.

13 (c) PRIORITIZATION.—In using amounts made avail-
14 able pursuant to subsection (a), a State shall prioritize
15 providing assistance to public water systems (as defined
16 in section 1401 of the Safe Drinking Water Act (42
17 U.S.C. 300f)) that have the greatest need with respect to
18 capacity, workforce, expertise, or resources to adequately
19 address cybersecurity vulnerabilities.

20 (d) ROLLOVER.—To the extent that any amounts au-
21 thorized to be appropriated under subsection (a) in a fiscal
22 year are not appropriated in that fiscal year, the amounts
23 are authorized to be appropriated in a subsequent fiscal
24 year, and shall remain available until expended.

TITLE II—CLEAN WATER INFRASTRUCTURE

SEC. 201. TREATMENT WORKS RISK AND RESILIENCE.

(a) IN GENERAL.—Title II of the Federal Water Pollution Control Act (33 U.S.C. 1281 et seq.) is amended by adding at the end the following:

“SEC. 228. TREATMENT WORKS RISK AND RESILIENCE.

“(a) DEFINITIONS.—In this section:

“(1) COVERED TREATMENT WORKS.—The term ‘covered treatment works’ means a treatment works that—

“(A) treats domestic sewage;

“(B) serves more than 10,000 persons; and

“(C) has a design flow rate of 1,000,000 gallons or more.

“(2) NATURAL HAZARD.—The term ‘natural hazard’ means a natural event that threatens the functioning of a treatment works, including an earthquake, tornado, flood, hurricane, wildfire, and hydrologic changes.

“(3) RESILIENCE.—The term ‘resilience’ means the ability of a treatment works or an asset of a treatment works to adapt to, or withstand the effects of, a malevolent act or natural hazard without interruption to the function of the treatment works

1 or asset or, if the function is interrupted, to rapidly
2 return to a normal operating condition.

3 “(4) STATE.—

4 “(A) IN GENERAL.—The term ‘State’
5 means a State that has assumed primary en-
6 forcement responsibility pursuant to section
7 229(e).

8 “(B) ENFORCEMENT BY THE ADMINIS-
9 TRATOR.—If a State has not assumed primary
10 enforcement responsibility pursuant to section
11 229(e), the term ‘State’ shall, for purposes of
12 obligations of the State under this subsection,
13 be considered to be a reference to the Adminis-
14 trator.

15 “(b) RISK AND RESILIENCE ASSESSMENTS.—

16 “(1) IN GENERAL.—Each covered treatment
17 works shall conduct an assessment of the risks to,
18 and resilience of, the covered treatment works.

19 “(2) REQUIREMENTS.—An assessment under
20 paragraph (1)—

21 “(A) shall include an assessment of—

22 “(i) the risk to the covered treatment
23 works from malevolent acts and natural
24 hazards;

1 “(ii) the resilience of collection sys-
2 tems, pipes and constructed conveyances,
3 physical barriers, treatment, and storage,
4 discharge, and reuse facilities that are uti-
5 lized by the covered treatment works;

6 “(iii) the monitoring practices of the
7 covered treatment works;

8 “(iv) the financial infrastructure of
9 the covered treatment works;

10 “(v) the use, storage, or handling of
11 various chemicals by the covered treatment
12 works;

13 “(vi) the operation and maintenance
14 of the covered treatment works; and

15 “(vii) using a method approved by the
16 applicable State, the risks to electronic,
17 computer, or other automated systems for
18 the purpose of identifying significant cy-
19 bersecurity risks that have the potential to
20 cause the impacts described in subpara-
21 graph (A) or (B) of paragraph (3); and

22 “(B) may include an evaluation of capital
23 and operational needs for risk and resilience
24 management for the covered treatment works.

1 “(3) BASELINE INFORMATION.—The Adminis-
 2 trator, not later than 1 year after the date of enact-
 3 ment of this section, after consultation with appro-
 4 priate departments and agencies of the Federal Gov-
 5 ernment and with State and local governments, shall
 6 provide baseline information on malevolent acts of
 7 relevance to covered treatment works, which shall in-
 8 clude consideration of acts that may—

9 “(A) substantially disrupt the ability of a
 10 covered treatment works to provide safe and re-
 11 liable collection, storage, treatment, recycling,
 12 and reclamation of municipal sewage or indus-
 13 trial wastes; or

14 “(B) otherwise present significant public
 15 health or economic concerns to the community
 16 served by a covered treatment works.

17 “(4) REVIEW AND REVISION.—

18 “(A) IN GENERAL.—Each covered treat-
 19 ment works shall, not less frequently than once
 20 every 5 years, review and, if necessary, revise
 21 the assessment.

22 “(B) CERTIFICATION TO THE ADMINIS-
 23 TRATOR OR STATE.—On completion of the re-
 24 view under subparagraph (A), a covered treat-
 25 ment works shall submit to the applicable State

1 a certification that the covered treatment works
2 has reviewed and, if applicable, revised the as-
3 sessment.

4 “(c) EMERGENCY RESPONSE PLAN.—

5 “(1) IN GENERAL.—Each covered treatment
6 works shall prepare an emergency response plan that
7 incorporates findings of the assessment conducted
8 under subsection (b) for that covered treatment
9 works (or any revisions to that assessment).

10 “(2) REQUIRED INCLUSIONS.—The emergency
11 response plan of a covered treatment works under
12 paragraph (1) shall include—

13 “(A) strategies and resources to improve
14 the resilience of the covered treatment works,
15 including the physical security of the covered
16 treatment works;

17 “(B) plans and procedures that can be im-
18 plemented, and identification of equipment that
19 can be utilized, in the event of a malevolent act
20 or natural hazard that threatens the ability of
21 the covered treatment works to collect, store,
22 treat, recycle, and reclaim municipal sewage or
23 industrial wastes;

24 “(C) actions, procedures, and equipment
25 that can obviate or significantly lessen the im-

1 pact of a malevolent act or natural hazard on
 2 the public health and the collection, storage,
 3 treatment, recycling, and reclamation of munic-
 4 ipal sewage or industrial wastes;

5 “(D) strategies that can be used to aid in
 6 the detection of malevolent acts or natural haz-
 7 ards that threaten the security or resilience of
 8 the covered treatment works; and

9 “(E) countermeasures that the covered
 10 treatment works intends to adopt or, if already
 11 in use, maintain to mitigate the significant cy-
 12 bersecurity risks identified under subsection
 13 (b)(2)(A)(vii), including a schedule the covered
 14 treatment works intends to follow to adopt any
 15 countermeasures not already in use by the cov-
 16 ered treatment works.

17 “(3) REVISION.—A covered treatment works
 18 shall review and, as necessary, revise the emergency
 19 response plan prepared under this subsection not
 20 less frequently than once every 5 years.

21 “(d) SUBMISSION AND APPROVAL OF ASSESSMENTS
 22 AND PLANS.—

23 “(1) SUBMISSION.—

24 “(A) IN GENERAL.—Beginning not later
 25 than 1 year after the date on which the Admin-

1 istrator provides baseline information under
 2 subsection (b)(3), each covered treatment works
 3 shall, during a cybersecurity assessment pursu-
 4 ant to section 229(b)(2)(A), provide to the ap-
 5 plicable State—

6 “(i) the portion of the assessment pre-
 7 pared under subsection (b) that is de-
 8 scribed in paragraph (2)(A)(vii) of that
 9 subsection (including any revision to that
 10 portion of the assessment); and

11 “(ii) the portion of the emergency re-
 12 sponse plan prepared under subsection (c)
 13 that is described in paragraph (2)(E) of
 14 that subsection (including any revision to
 15 that portion of the emergency response
 16 plan).

17 “(B) LIMITATION.—Neither the Adminis-
 18 trator nor a State may require the submission
 19 of any portion of an assessment under sub-
 20 section (a) or an emergency response plan
 21 under subsection (b) that is not described in
 22 subparagraph (A).

23 “(2) REVIEW; APPROVAL.—

24 “(A) IN GENERAL.—A State shall—

1 “(i) review the portions of the assess-
2 ments and emergency response plans of
3 covered treatment works submitted pursu-
4 ant to paragraph (1)(A) for conformity
5 with the requirements of this section and
6 section 229; and

7 “(ii)(I) approve of the portions of an
8 assessment and emergency response plan
9 submitted pursuant to paragraph (1)(A);
10 or

11 “(II) disapprove of the portions of an
12 assessment or emergency response plan
13 submitted pursuant to paragraph (1)(A) if
14 the Administrator or the State, as applica-
15 ble, determines that—

16 “(aa) the submitted portions of
17 the assessment or emergency response
18 plan are missing, incomplete, or fail to
19 conform with the requirements of this
20 section; or

21 “(bb) the submitted portions of
22 the assessment or emergency response
23 plan fail to provide for cybersecurity
24 resilience in accordance with the base-
25 line cybersecurity standards estab-

lished by the Administrator under section 229(c).

“(B) ENFORCEMENT.—A State may use appropriate enforcement mechanisms under this Act or the appropriate State authority to remedy noncompliance, as described in items (aa) and (bb) of subparagraph (A)(ii)(II), under this subsection.

“(3) SUBMITTED DOCUMENTATION.—

“(A) APPLICABILITY OF FOIA.—Any information submitted under this subsection shall be exempt from disclosure under section 552(b)(3) of title 5, United States Code (commonly known as the ‘Freedom of Information Act’), and any provision of State, Tribal, or local freedom of information law, open government law, open meetings law, open records law, sunshine law, or similar law requiring disclosure of information or records.

“(B) TREATMENT OF DOCUMENTATION.—

“(i) PROTOCOL DEVELOPMENT.—Not later than 180 days after the date of enactment of the Water Cyber Shield Act of 2026 and before any cybersecurity assessments are carried out pursuant to section

1 229(b)(2)(A), the Administrator, in con-
2 sultation with appropriate Federal law en-
3 forcement and intelligence officials, shall
4 develop such protocols as are necessary to
5 protect any information provided under
6 paragraph (1)(A) to the State.

7 “(ii) REQUIREMENTS FOR PRO-
8 TOCOL.—The protocol developed under
9 clause (i) shall ensure that—

10 “(I) each copy of the portions of
11 an assessment and emergency re-
12 sponse plan submitted pursuant to
13 paragraph (1)(A) are kept in a secure
14 location;

15 “(II) only individuals designated
16 by the applicable State may have ac-
17 cess to copies of the portions of the
18 assessment and emergency response
19 plan submitted pursuant to paragraph
20 (1)(A); and

21 “(III) no copy of the portions of
22 the assessment and emergency re-
23 sponse plan submitted pursuant to
24 paragraph (1)(A) shall be made avail-
25 able to anyone other than an indi-

1 vidual designated by the applicable
2 State.

3 “(iii) SAVINGS PROVISION.—Nothing
4 in this subparagraph authorizes any person
5 to withhold any information from Congress
6 or from a committee or subcommittee of
7 Congress.

8 “(4) APPLICABILITY OF FOIA.—Any findings or
9 plans (including revisions and any related agency
10 records and information that is designated as De-
11 partment of Defense critical infrastructure security
12 information under section 130e(b) of title 10, United
13 States Code) submitted under this subsection shall
14 be exempt from disclosure under section 552(b)(3)
15 of title 5, United States Code (commonly known as
16 the ‘Freedom of Information Act’), and any provi-
17 sion of State, Tribal, or local freedom of information
18 law, open government law, open meetings law, open
19 records law, sunshine law, or similar law requiring
20 disclosure of information or records.

21 “(e) COORDINATION.—A covered treatment works
22 shall, to the extent practicable, coordinate with existing
23 local planning committees established pursuant to the
24 Emergency Planning and Community Right-To-Know Act
25 of 1986 (42 U.S.C. 11001 et seq.) when preparing or re-

1 vising an assessment or emergency response plan under
2 this section.

3 “(f) RECORD MAINTENANCE.—Each covered treat-
4 ment works shall maintain a copy of the assessment con-
5 ducted under subsection (b) and the emergency response
6 plan prepared under subsection (c) (including any revised
7 assessment or plan) for 5 years after the date on which
8 that assessment or plan is approved by the applicable
9 State under this section.

10 “(g) GUIDANCE TO SMALL TREATMENT WORKS.—
11 The Administrator shall provide guidance and technical
12 assistance to treatment works that are not covered treat-
13 ment works on how to conduct resilience assessments, pre-
14 pare emergency response plans, and address threats from
15 malevolent acts and natural hazards that threaten to dis-
16 rupt the collection, storage, treatment, recycling, and rec-
17 lamation of municipal sewage or industrial wastes or sig-
18 nificantly affect the public health.”.

19 (b) FEDERAL ENFORCEMENT.—Section 309 of the
20 Federal Water Pollution Control Act (33 U.S.C. 1319) is
21 amended in each of subsections (a), (c), (d), and (g) by
22 inserting “228(d),” before “301,” each place it appears.

1 **SEC. 202. CYBERSECURITY REQUIREMENTS FOR TREAT-**
 2 **MENT WORKS.**

3 (a) IN GENERAL.—Title II of the Federal Water Pol-
 4 lution Control Act (33 U.S.C. 1281 et seq.) (as amended
 5 by section 201(a)) is amended by adding at the end the
 6 following:

7 **“SEC. 229. CYBERSECURITY REQUIREMENTS.**

8 “(a) DEFINITIONS.—In this section:

9 “(1) COVERED TREATMENT WORKS.—The term
 10 ‘covered treatment works’ has the meaning given the
 11 term in section 228(a).

12 “(2) CYBERSECURITY INCIDENT.—The term
 13 ‘cybersecurity incident’ means a malicious act or
 14 suspicious event that disrupts, or attempts to dis-
 15 rupt, the operation of programmable electronic de-
 16 vices and communication networks, including hard-
 17 ware, software, and data that are essential to the cy-
 18 bersecurity resilience of a treatment works.

19 “(3) CYBERSECURITY RESILIENCE.—The term
 20 ‘cybersecurity resilience’ means the ability of a treat-
 21 ment works to adapt to or withstand the effects of
 22 a cybersecurity incident without interruption to the
 23 treatment works’s function, or if the function is in-
 24 terrupted, to rapidly return to a normal operating
 25 condition.

26 “(4) STATE.—

1 “(A) IN GENERAL.—Except for subsection
2 (e), the term ‘State’ means a State that has as-
3 sumed primary enforcement responsibility pur-
4 suant to subsection (e).

5 “(B) ENFORCEMENT BY THE ADMINIS-
6 TRATOR.—If a State has not assumed primary
7 enforcement responsibility pursuant to sub-
8 section (e), the term ‘State’ shall, for purposes
9 of obligations of the State under this section
10 (except for subsection (e)), be considered to be
11 a reference to the Administrator.

12 “(b) CYBERSECURITY ASSESSMENTS.—

13 “(1) ASSESSMENTS REQUIRED.—

14 “(A) IN GENERAL.—A State shall carry
15 out cybersecurity assessments of a covered
16 treatment works in accordance with this para-
17 graph.

18 “(B) EVALUATION OF ADEQUACY.—For a
19 covered treatment works subject to a cybersecu-
20 rity assessment under subparagraph (A), if the
21 covered treatment works uses operational tech-
22 nology, the State shall evaluate the adequacy of
23 the cybersecurity of the operational technology,
24 and information and communications tech-
25 nology that is connected to the operational tech-

nology, against the baseline cybersecurity standards promulgated by the Administrator under subsection (c).

“(C) REVIEW OF ASSESSMENTS AND PLANS.—In carrying out a cybersecurity assessment required under subparagraph (A), a covered treatment works shall provide, and the State shall review, the portions of the risk and resilience assessments of the covered treatment works under section 228(b) and the emergency response plans of the covered treatment works under section 228(c) submitted under section 228(d)(1)(A).

“(D) INSPECTIONS.—In carrying out cybersecurity assessments under this paragraph, a State shall carry out inspections of a representative sample of covered treatment works each year, which sampling shall be informed by risk-based considerations, subject to the condition that the scope of the inspection is limited to the systems of the covered treatment works necessary to meet the requirements of this paragraph.

“(2) VIOLATIONS.—If a State identifies a violation of the baseline cybersecurity standards estab-

1 lished by the Administrator under subsection (c)
 2 while conducting an assessment under paragraph
 3 (3), the State shall take appropriate steps to ensure
 4 that the covered treatment works addresses the vio-
 5 lation and use mechanisms, including enforcement,
 6 to correct those violations.

7 “(3) SUBMISSION TO EPA.—

8 “(A) IN GENERAL.—A State shall annually
 9 submit to the Administrator a report that sum-
 10 marizes the performance of the covered treat-
 11 ment works of the State for each cybersecurity
 12 performance metric established by the Adminis-
 13 trator under subsection (d)(1) based on the re-
 14 view by the State of risk and resilience assess-
 15 ments pursuant to paragraph (1)(C).

16 “(B) REQUIREMENT.—A report submitted
 17 under subparagraph (A) shall not identify any
 18 specific treatment works and shall include only
 19 aggregations of data.

20 “(4) TECHNICAL ASSISTANCE.—The Adminis-
 21 trator shall, on request of a covered treatment
 22 works, provide guidance and technical assistance to
 23 the covered treatment works with respect to—

24 “(A) implementing any requirement under
 25 this section or section 228; and

1 “(B) enhancing cybersecurity resilience.

2 “(c) BASELINE CYBERSECURITY STANDARDS.—

3 “(1) IN GENERAL.—The Administrator shall by
4 rulemaking establish baseline cybersecurity stand-
5 ards that shall serve as requirements to provide for
6 the cybersecurity resilience of a covered treatment
7 works.

8 “(2) REQUIREMENTS.—In developing and es-
9 tablishing the baseline cybersecurity standards under
10 paragraph (1), the Administrator shall, at a min-
11 imum—

12 “(A) work in conjunction with the Director
13 of the Cybersecurity and Infrastructure Secu-
14 rity Agency and the Director of the National
15 Institute of Standards and Technology;

16 “(B) develop the baseline cybersecurity
17 standards in collaboration with covered treat-
18 ment works of various sizes and capacities to
19 ensure that feedback from a variety of covered
20 treatment works is considered during the devel-
21 opment of the baseline cybersecurity standards;

22 “(C) ensure that best practices and guide-
23 lines that already exist in the water sector at
24 the time of the development of the baseline cy-

bersecurity standards inform the development
of the baseline cybersecurity standards;

“(D) establish a technical advisory committee to provide input with respect to, review, and refine the baseline cybersecurity standards throughout the development process, which shall, at a minimum, include—

“(i) representatives from covered treatment works of various sizes;

“(ii) professional water associations;

“(iii) cybersecurity experts;

“(iv) a representative from a relevant voluntary consensus standards body, as described in section 12(d)(1) of the National Technology Transfer and Advancement Act of 1995 (15 U.S.C. 272 note; Public Law 104–113); and

“(v) a representative from an information technology or operational technology service provider that provides cybersecurity services to covered treatment works; and

“(E) consult with the States.

1 “(3) CONSIDERATION OF VARIED CAPACITY
2 AND RISK.—In developing the baseline cybersecurity
3 standards under paragraph (1), the Administrator—

4 “(A) shall ensure that the baseline cyberse-
5 curity standards account for the varied capacity
6 and risk of all covered treatment works; and

7 “(B) may establish different baseline cy-
8 bersecurity standards for different categories of
9 treatment works subject to assessments under
10 subsection (b) based on capacity or risk.

11 “(d) CYBERSECURITY PERFORMANCE METRICS.—

12 “(1) ESTABLISHMENT OF METRICS.—

13 “(A) IN GENERAL.—Not later than 2 years
14 after the date of enactment of this section, the
15 Administrator shall establish cybersecurity per-
16 formance metrics (referred to in this subsection
17 as the ‘cybersecurity performance metrics’) to
18 be used by the Administrator to measure or as-
19 sess how well the sector of treatment works in
20 the United States is making progress on imple-
21 menting cybersecurity best practices.

22 “(B) ASSESSMENT; REPORT.—The Admin-
23 istrator shall, not less frequently than once
24 every 4 years—

1 “(i) assess the sector of treatment
2 works in the United States using cyberse-
3 curity performance metrics; and

4 “(ii) submit to Congress and make
5 publicly available a report describing, on a
6 generalized, sector-wide basis, the state of
7 treatment works sector performance using
8 the assessment carried out under clause
9 (i).

10 “(2) PROVISION OF INFORMATION.—Notwith-
11 standing any other provision of law, a treatment
12 works may, at the discretion of the treatment works
13 and for the purpose of developing sector-wide risk
14 assessments and performance metrics to measure
15 how treatment works are making progress in devel-
16 oping and implementing cybersecurity best practices,
17 provide to the Administrator, and the Administrator
18 may accept, information that would assist the Ad-
19 ministrator in the development and maintenance of
20 cybersecurity performance metrics.

21 “(e) ENFORCEMENT; STATE ASSUMPTION OF DU-
22 TIES.—

23 “(1) IN GENERAL.—This section and section
24 228 shall be enforced by the Administrator unless a

1 State assumes primary enforcement responsibility
2 pursuant to this subsection.

3 “(2) APPLICATION.—A State seeking to assume
4 primary enforcement responsibility pursuant to this
5 subsection shall submit to the Administrator an ap-
6 plication at such time, in such manner, and con-
7 taining such information as the Administrator may
8 by regulation require.

9 “(3) DETERMINATION.—On receiving an appli-
10 cation described in paragraph (2) from a State, the
11 Administrator shall, based on that application, de-
12 termine whether the State—

13 “(A) has adopted and is implementing ade-
14 quate procedures for the enforcement of re-
15 quirements that are no less stringent than those
16 under this section and section 228;

17 “(B) has adopted authority and has suffi-
18 cient capacity to impose enforcement remedies
19 in line with those prescribed under this title;

20 “(C) has sufficient capacity and personnel
21 with sufficient expertise to perform cybersecu-
22 rity assessments and conduct reviews of risk
23 and resilience assessments and emergency re-
24 sponse plans under section 228; and

1 “(D) has sufficient security mechanisms in
2 place to prevent any unsanctioned disclosure or
3 dissemination of risk and resilience assess-
4 ments, emergency response plans, and any
5 other information provided by a covered treat-
6 ment works, in alignment with the protocols de-
7 veloped by the Administrator under section
8 228(d)(3)(B)(i).

9 “(4) TIMELINE.—Not later than 180 days after
10 the date on which the Administrator receives an ap-
11 plication described in paragraph (2), the Adminis-
12 trator shall—

13 “(A) if the Administrator determines that
14 the State meets each requirement described in
15 paragraph (3), grant the application; or

16 “(B) if the Administrator determines that
17 the State fails to meet 1 or more of the require-
18 ments described in paragraph (3), deny the ap-
19 plication.

20 “(5) REVOCATION OF PRIMARY ENFORCEMENT
21 RESPONSIBILITY.—The Administrator may, as ap-
22 propriate, revoke an assumption of primary enforce-
23 ment responsibility pursuant to this subsection if the
24 Administrator determines that a State no longer

1 meets 1 or more requirements described in para-
 2 graph (3).

3 “(6) REGULATIONS REQUIRED.—The Adminis-
 4 trator shall promulgate regulations carrying out this
 5 subsection not later than 1 year after the date of en-
 6 actment of this section, which shall include—

7 “(A) the requirements for an application
 8 described in paragraph (2);

9 “(B) the period for which a State may as-
 10 sume primary enforcement responsibility pursu-
 11 ant to this subsection before renewal; and

12 “(C) the manner by which the Adminis-
 13 trator may revoke primary enforcement respon-
 14 sibility pursuant to paragraph (5).

15 “(7) SAVINGS PROVISION.—An assumption of
 16 primary enforcement responsibility pursuant to this
 17 subsection shall be separate from any responsibility
 18 otherwise assumed under this Act.”.

19 (b) INSPECTIONS.—Section 308(a) of the Federal
 20 Water Pollution Control Act (33 U.S.C. 1318(a)) is
 21 amended, in the matter preceding subparagraph (A)—

22 (1) by striking “or (4) carrying” and inserting
 23 “(4) carrying”; and

1 (2) by striking “504 of this Act—” and insert-
 2 ing “504; or (5) carrying out requirements under
 3 section 229—”.

4 (c) **FEDERAL ENFORCEMENT.**—Section 309 of the
 5 Federal Water Pollution Control Act (33 U.S.C. 1319) (as
 6 amended by section 201(b)) is amended in each of sub-
 7 sections (a), (c), (d), and (g) by inserting “229,” before
 8 “301,” each place it appears.

9 **SEC. 203. CLEAN WATER SECURITY ASSISTANCE.**

10 (a) **AUTHORIZATION OF APPROPRIATIONS.**—In addi-
 11 tion to any amounts authorized to be appropriated under
 12 section 607 of the Federal Water Pollution Control Act
 13 (33 U.S.C. 1387), there is authorized to be appropriated
 14 \$300,000,000 for each of fiscal years 2027 through 2032
 15 for the purposes of helping treatment works (as defined
 16 in section 212 of that Act (33 U.S.C. 1292)) build cyber-
 17 security resilience (as defined in section 229 of the Fed-
 18 eral Water Pollution Control Act) and identifying and
 19 mitigating cybersecurity vulnerabilities, including those in-
 20 cluded in risk and resilience assessments and emergency
 21 response plans prepared pursuant to section 228 of that
 22 Act.

23 (b) **GUIDANCE.**—The Administrator of the Environ-
 24 mental Protection Agency may issue guidance to deter-
 25 mine specific criteria for eligible uses of the amounts made

1 available under subsection (a) that further the purposes
2 described in that subsection.

3 (c) PRIORITIZATION.—In using amounts made avail-
4 able pursuant to subsection (a), a State shall prioritize
5 providing assistance to treatment works (as defined in sec-
6 tion 212 of the Federal Water Pollution Control Act (33
7 U.S.C. 1292)) that have the greatest need with respect
8 to capacity, workforce, expertise, or resources to ade-
9 quately address cybersecurity vulnerabilities.

10 (d) ROLLOVER.—To the extent that any amounts au-
11 thorized to be appropriated under subsection (a) in a fiscal
12 year are not appropriated in that fiscal year, the amounts
13 are authorized to be appropriated in a subsequent fiscal
14 year, and shall remain available until expended.

15 **TITLE III—CYBER INCIDENT** 16 **REPORTING OBLIGATIONS**

17 **SEC. 301. CYBER INCIDENT REPORTING.**

18 Subtitle D of title XXII of the Homeland Security
19 Act of 2002 (6 U.S.C. 681 et seq.) is amended—

20 (1) in section 2240 (6 U.S.C. 681), by striking
21 paragraph (4) and inserting the following:

22 “(4) COVERED ENTITY.—The term ‘covered en-
23 tity’—

24 “(A) means an entity in a critical infra-
25 structure sector, as defined in Presidential Pol-

1 icy Directive 21, that satisfies the definition es-
 2 tablished by the Director in the final rule issued
 3 pursuant to section 2242(b); and

4 “(B) includes—

5 “(i) a community water system (as
 6 defined in section 1401 of the Safe Drink-
 7 ing Water Act (42 U.S.C. 300f)) that
 8 serves a population of greater than 3,300
 9 persons; and

10 “(ii) a covered treatment works (as
 11 defined in section 228(a) of the Federal
 12 Water Pollution Control Act).”;

13 (2) in section 2242(a) (6 U.S.C. 681b(a)), by
 14 adding at the end the following:

15 “(8) TRANSMISSION TO EPA.—The Agency shall
 16 submit to the Administrator of the Environmental
 17 Protection Agency a copy of each report submitted
 18 to the Agency under paragraph (1), (2), or (3).”;
 19 and

20 (3) in section 2244(f) (6 U.S.C. 681d(f))—

21 (A) by striking “This section” and insert-
 22 ing the following:

23 “(1) IN GENERAL.—Except as provided in para-
 24 graph (2), this section”; and

25 (B) by adding at the end the following:

1 “(2) EXCEPTION.—This section shall apply to a
2 State, local, Tribal, or territorial government entity
3 that is required to submit a report under section
4 2242(a) with respect to a community water system
5 or covered treatment works, as defined in clauses (i)
6 and (ii), respectively, of section 2240(4)(B), that is
7 owned or operated by the State, local, Tribal or ter-
8 ritorial government entity.”.

○