119TH CONGRESS
2D SESSION

S. _____

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

Mr. SCHIFF introduced the following bill; which was read twice and referred to the Committee on _____

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.

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

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the ''Water Cyber Shield Act of 2026''.

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

TITLE I—DRINKING WATER INFRASTRUCTURE

SEC. 101. COMMUNITY WATER SYSTEM RISK AND RESILIENCE.

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

(1) in subsection (a)—

(A) in paragraph (1)(A)—

(i) in clause (ii), by striking ''storage and distribution facilities, electronic, computer, or other automated systems (including the security of such systems) which'' and inserting ''and storage and distribution facilities that'';

(ii) in clause (v), by striking ''and'' at the end; and

(iii) by adding at the end the following:

"(vii) using a method approved by the applicable State, the risks to electronic, computer, or other automated systems for the purpose of identifying significant cybersecurity risks that have the potential to cause the impacts described in subparagraph (A) or (B) of paragraph (2); and"; and

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

"(3) REVIEW AND REVISION.—

"(A) IN GENERAL.—Each community water system described in paragraph (1) shall, not less frequently than once every 5 years, review and, if necessary, revise the assessment.

"(B) CERTIFICATION TO THE ADMINISTRATOR OR STATE.—On completion of the review under subparagraph (A), a community water system described in paragraph (1) shall submit to the applicable State a certification that the community water system has reviewed and, if applicable, revised the assessment.";

(2) in subsection (b)—

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

(B) in the matter preceding subparagraph (A) (as so redesignated), by striking ''Each community water system'' in the first sentence and all that follows through ''The emergency response plan'' in the third sentence and inserting the following:

''(1) IN GENERAL.—Each community water system serving a population greater than 3,300 shall prepare an emergency response plan that incorporates findings of the assessment conducted under subsection (a) for that community water system (or any revisions to that assessment).

''(2) REQUIRED INCLUSIONS.—The emergency response plan of a community water system under paragraph (1)'';

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

(i) in subparagraph (A) (as so redesignated), by striking ''and cybersecurity'';

(ii) in subparagraph (C) (as so redesignated), by striking ''and'' at the end;

(iii) in subparagraph (D) (as so redesignated), by striking the period at the end and inserting ''; and''; and

(iv) by adding at the end the following:

''(E) countermeasures that the system intends to adopt or, if already in use, maintain to mitigate the significant cybersecurity risks identified under subsection (a)(1)(A)(vii), including a schedule the system intends to follow to adopt any countermeasures not already in use by the system.''; and

(D) by adding at the end the following:

''(3) REVIEW; REVISION.—A community water system serving a population greater than 3,300 shall review and, as necessary, revise the emergency response plan prepared under this subsection not less frequently than once every 5 years.'';

(3) by striking subsection (f);

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

(5) by inserting after subsection (b) the following:

''(c) SUBMISSION AND APPROVAL OF ASSESSMENTS AND PLANS.—

"(1) SUBMISSION.—

"(A) IN GENERAL.—Each community water system subject to subsections (a) and (b) shall, during a cybersecurity assessment pursuant to section 1433A(b)(1)(A), provide to the applicable State—

"(i) the portion of the assessment prepared under subsection (a) that is described in paragraph (1)(A)(vii) of that subsection (including any revision to that portion of the assessment); and

"(ii) the portion of the emergency response plan prepared under subsection (b) that is described in paragraph (2)(E) of that subsection (including any revision to that portion of the emergency response plan).

"(B) LIMITATION.—Neither the Administrator nor a State may require the submission of any portion of an assessment under subsection (a) or an emergency response plan under subsection (b) that is not described in subparagraph (A).

"(2) REVIEW; APPROVAL.—

"(A) IN GENERAL.—A State shall—

"(i) review the portions of the assessments and emergency response plans of community water systems submitted pursuant to paragraph (1)(A) for conformity with the requirements of this section and section 1433A; and

"(ii)(I) approve of the portions of an assessment and emergency response plan submitted pursuant to paragraph (1)(A); or

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

"(aa) the submitted portions of the assessment or emergency response plan are missing, incomplete, or fail to conform with the requirements of this section or section 1433A; or

"(bb) the submitted portions of the assessment or emergency response plan fail to provide for cybersecurity resilience in accordance with the baseline cybersecurity standards estab-

lished by the Administrator under section 1433A(c).

''(B) ENFORCEMENT.—A State may use appropriate enforcement mechanisms under this title 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

1433A(b)(1)(A), the Administrator, in consultation with appropriate Federal law enforcement and intelligence officials, shall develop such protocols as are necessary to protect any information provided under paragraph (1)(A) to the State.

''(ii) REQUIREMENTS FOR PROTOCOL.—The protocol developed under clause (i) shall ensure that—

''(I) each copy of the portions of an assessment and emergency response plan submitted pursuant to paragraph (1)(A) are kept in a secure location;

''(II) only individuals designated by the applicable State may have access to copies of the portions of the assessment and emergency response plan submitted pursuant to paragraph (1)(A); and

''(III) no copy of the portions of the assessment and emergency response plan submitted pursuant to paragraph (1)(A) shall be made available to anyone other than an indi-

vidual designated by the applicable State.

''(iii) SAVINGS PROVISION.—Nothing in this subparagraph authorizes any person to withhold any information from Congress or from a committee or subcommittee of Congress.'';

(6) in subsection (e) (as so redesignated), by striking ''a certification of such assessment or plan is submitted to the Administrator'' and inserting ''an assessment or plan is submitted to the applicable State,''; and

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

''(h) DEFINITIONS.—In this section:

''(1) NATURAL HAZARD.—The term 'natural hazard' means a natural event that threatens the functioning of a community water system, including an earthquake, tornado, flood, hurricane, wildfire, and hydrologic changes.

''(2) RESILIENCE.—The term 'resilience' means the ability of a community water system or an asset of a community water system to adapt to or withstand the effects of a malevolent act or natural hazard 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-

vices and communication networks, including hardware, software, and data that are essential to the cybersecurity resilience of a public water system.

''(2) CYBERSECURITY RESILIENCE.—The term 'cybersecurity resilience' means the ability of a public water system to adapt to or withstand the effects of a cybersecurity incident without interruption to the public water system's function, or if the function is interrupted, to rapidly return to a normal operating condition.

''(3) STATE.—

''(A) IN GENERAL.—Except for subsection (e), the term 'State' means a State that has assumed primary enforcement responsibility pursuant to subsection (e).

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

''(b) CYBERSECURITY ASSESSMENTS.—

''(1) ASSESSMENTS REQUIRED.—

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

"(B) EVALUATION OF ADEQUACY.—For a public water system subject to a cybersecurity assessment under subparagraph (A), if the public water system uses operational technology, the State shall evaluate the adequacy of the cybersecurity of the operational technology, and information and communications technology that is connected to the operational technology, 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 public water system shall provide, and the State shall review, the portions of the risk and resilience assessments of the public water system under section 1433(a) and the emergency response plans of the public water system under section 1433(b) submitted under section 1433(c)(1)(A).

"(D) INSPECTIONS.—In carrying out cybersecurity assessments under this paragraph, a State shall carry out inspections of a representative sample of public water systems 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 public water system necessary to meet the requirements of this paragraph.

"(2) VIOLATIONS.—If a State identifies a violation of the baseline cybersecurity standards established by the Administrator under subsection (c) while conducting an assessment under paragraph (1), the State shall take appropriate steps to ensure that the public water system addresses the violation and use mechanisms, including enforcement, for failures to correct those violations.

"(3) SUBMISSION TO EPA.—

"(A) IN GENERAL.—A State shall annually submit to the Administrator a report that summarizes the performance of the public water systems of the State for each cybersecurity performance metric established by the Administrator under subsection (d)(1) based on the re-

view by the State of risk and resilience assessments pursuant to paragraph (1)(C).

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

''(4) TECHNICAL ASSISTANCE.—The Administrator shall, on request of a public water system, provide guidance and technical assistance to the public water system with respect to—

''(A) implementing any requirement under this section or section 1433; and

''(B) enhancing cybersecurity resilience.

''(c) BASELINE CYBERSECURITY STANDARDS.—

''(1) IN GENERAL.—The Administrator shall by rulemaking establish baseline cybersecurity standards that shall serve as requirements to provide for the cybersecurity resilience of a public water system.

''(2) REQUIREMENTS.—In developing and establishing the baseline cybersecurity standards under paragraph (1), the Administrator shall, at a minimum—

''(A) work in conjunction with the Director of the Cybersecurity and Infrastructure Secu-

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

"(B) develop the baseline cybersecurity standards in collaboration with public water systems of various sizes and capacities to ensure that feedback from a variety of public water systems is considered during the development of the baseline cybersecurity standards;

"(C) ensure that best practices and guidelines that already exist in the water sector at the time of the development of the baseline cybersecurity 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 public water systems 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) representative from an information technology or operational technology service provider that provides cybersecurity 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 cybersecurity standards account for the varied capacity and risk of all public water systems; and

"(B) may establish different baseline cybersecurity 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 performance metrics (referred to in this subsection as the 'cybersecurity performance metrics') to

be used by the Administrator to measure or assess how well the sector of public water systems in the United States is making progress on implementing cybersecurity best practices.

''(B) ASSESSMENT; REPORT.—The Administrator shall, not less frequently than once every 4 years—

''(i) assess the sector of public water systems in the United States using the cybersecurity performance metrics; and

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

''(2) PROVISION OF INFORMATION.—Notwithstanding any other provision of law, a public water system may, at the discretion of the public water system and for the purpose of developing sector-wide risk assessments and performance metrics to measure how public water systems are making progress in developing and implementing cybersecurity best practices, provide to the Administrator, and the Administrator may accept, information that would as-

sist the Administrator in the development and maintenance of the cybersecurity performance metrics.

''(e) ENFORCEMENT; STATE ASSUMPTION OF DUTIES.—

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

''(2) APPLICATION.—A State seeking to assume primary enforcement responsibility pursuant to this subsection shall submit to the Administrator an application at such time, in such manner, and containing such information as the Administrator may by regulation require.

''(3) DETERMINATION.—On receiving an application described in paragraph (2) from a State, the Administrator shall, based on that application, determine whether the State—

''(A) has adopted and is implementing adequate procedures for the enforcement of requirements that are no less stringent than those under this section and section 1433;

''(B) has adopted authority and has sufficient capacity to impose enforcement remedies in line with those prescribed under this title;

"(C) has sufficient capacity and personnel with sufficient expertise to perform cybersecurity assessments and conduct reviews of risk and resilience assessments and emergency response plans under section 1433; and

"(D) has sufficient security mechanisms in place to prevent any unsanctioned disclosure or dissemination of risk and resilience assessments, emergency response plans, and any other information provided by a public water system, in alignment with the protocols developed by the Administrator under section 1433(c)(3)(B)(i).

"(4) TIMELINE.—Not later than 180 days after the date on which the Administrator receives an application described in paragraph (2), the Administrator shall—

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

"(B) if the Administrator determines that the State fails to meet 1 or more of the requirements described in paragraph (3), deny the application.

''(5) REVOCATION OF PRIMARY ENFORCEMENT RESPONSIBILITY.—The Administrator may, as appropriate, revoke an assumption of primary enforcement responsibility pursuant to this subsection if the Administrator determines that a State no longer meets 1 or more requirements described in paragraph (3).

''(6) REGULATIONS REQUIRED.—The Administrator shall promulgate regulations carrying out this subsection not later than 1 year after the date of enactment of this section, which shall include—

''(A) the requirements for an application described in paragraph (2);

''(B) the period for which a State may assume primary enforcement responsibility pursuant to this subsection before renewal; and

''(C) the manner by which the Administrator may revoke primary enforcement responsibility pursuant to paragraph (5).

''(7) SAVINGS PROVISION.—An assumption of primary enforcement responsibility pursuant to this subsection shall be separate from any authority assumed under section 1413.''.

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

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

(1) by striking ''or (C) any'' and inserting ''(C) any'';

(2) by inserting ''or (D) a requirement to undergo an inspection under section 1433A(a)(2)(D),'' after ''subsection (a),''; and

(3) by striking ''or (C), is'' and inserting ''(C), or (D), is''.

(d) CONFORMING AMENDMENT.—Section 1413(a) of the Safe Drinking Water Act (42 U.S.C. 300g–2(a)) is amended, in the matter preceding paragraph (1), by inserting ''(except for sections 1433 and 1433A)'' after ''this title''.

SEC. 103. DRINKING WATER SECURITY ASSISTANCE.

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

tems (as defined in section 1401 of that Act (42 U.S.C. 300f)) build cybersecurity resilience (as defined in section 1433A(a)(1) of the Safe Drinking Water Act) and identifying and mitigating cybersecurity vulnerabilities, including those included in risk and resilience assessments and emergency response plans prepared pursuant to section 1433 of that Act (42 U.S.C. 300i–2).

(b) GUIDANCE.—The Administrator of the Environmental Protection Agency may issue guidance to determine specific criteria for eligible uses of the amounts made available under subsection (a) that further the purposes described in that subsection.

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

(d) ROLLOVER.—To the extent that any amounts authorized to be appropriated under subsection (a) in a fiscal year are not appropriated in that fiscal year, the amounts are authorized to be appropriated in a subsequent fiscal 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

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

''(4) STATE.—

''(A) IN GENERAL.—The term 'State' means a State that has assumed primary enforcement responsibility pursuant to section 229(e).

''(B) ENFORCEMENT BY THE ADMINISTRATOR.—If a State has not assumed primary enforcement responsibility pursuant to section 229(e), the term 'State' shall, for purposes of obligations of the State under this subsection, be considered to be a reference to the Administrator.

''(b) RISK AND RESILIENCE ASSESSMENTS.—

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

''(2) REQUIREMENTS.—An assessment under paragraph (1)—

''(A) shall include an assessment of—

''(i) the risk to the covered treatment works from malevolent acts and natural hazards;

"(ii) the resilience of collection systems, pipes and constructed conveyances, physical barriers, treatment, and storage, discharge, and reuse facilities that are utilized by the covered treatment works;

"(iii) the monitoring practices of the covered treatment works;

"(iv) the financial infrastructure of the covered treatment works;

"(v) the use, storage, or handling of various chemicals by the covered treatment works;

"(vi) the operation and maintenance of the covered treatment works; and

"(vii) using a method approved by the applicable State, the risks to electronic, computer, or other automated systems for the purpose of identifying significant cybersecurity risks that have the potential to cause the impacts described in subparagraph (A) or (B) of paragraph (3); and

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

"(3) BASELINE INFORMATION.—The Administrator, not later than 1 year after the date of enactment of this section, after consultation with appropriate departments and agencies of the Federal Government and with State and local governments, shall provide baseline information on malevolent acts of relevance to covered treatment works, which shall include consideration of acts that may—

"(A) substantially disrupt the ability of a covered treatment works to provide safe and reliable collection, storage, treatment, recycling, and reclamation of municipal sewage or industrial wastes; or

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

"(4) REVIEW AND REVISION.—

"(A) IN GENERAL.—Each covered treatment works shall, not less frequently than once every 5 years, review and, if necessary, revise the assessment.

"(B) CERTIFICATION TO THE ADMINISTRATOR OR STATE.—On completion of the review under subparagraph (A), a covered treatment works shall submit to the applicable State

a certification that the covered treatment works has reviewed and, if applicable, revised the assessment.

''(c) EMERGENCY RESPONSE PLAN.—

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

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

''(A) strategies and resources to improve the resilience of the covered treatment works, including the physical security of the covered treatment works;

''(B) plans and procedures that can be implemented, and identification of equipment that can be utilized, in the event of a malevolent act or natural hazard that threatens the ability of the covered treatment works to collect, store, treat, recycle, and reclaim municipal sewage or industrial wastes;

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

pact of a malevolent act or natural hazard on the public health and the collection, storage, treatment, recycling, and reclamation of municipal sewage or industrial wastes;

"(D) strategies that can be used to aid in the detection of malevolent acts or natural hazards that threaten the security or resilience of the covered treatment works; and

"(E) countermeasures that the covered treatment works intends to adopt or, if already in use, maintain to mitigate the significant cybersecurity risks identified under subsection (b)(2)(A)(vii), including a schedule the covered treatment works intends to follow to adopt any countermeasures not already in use by the covered treatment works.

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

"(d) SUBMISSION AND APPROVAL OF ASSESSMENTS AND PLANS.—

"(1) SUBMISSION.—

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

istrator provides baseline information under subsection (b)(3), each covered treatment works shall, during a cybersecurity assessment pursuant to section 229(b)(2)(A), provide to the applicable State—

"(i) the portion of the assessment prepared under subsection (b) that is described in paragraph (2)(A)(vii) of that subsection (including any revision to that portion of the assessment); and

"(ii) the portion of the emergency response plan prepared under subsection (c) that is described in paragraph (2)(E) of that subsection (including any revision to that portion of the emergency response plan).

"(B) LIMITATION.—Neither the Administrator nor a State may require the submission of any portion of an assessment under subsection (a) or an emergency response plan under subsection (b) that is not described in subparagraph (A).

"(2) REVIEW; APPROVAL.—

"(A) IN GENERAL.—A State shall—

"(i) review the portions of the assessments and emergency response plans of covered treatment works submitted pursuant to paragraph (1)(A) for conformity with the requirements of this section and section 229; and

"(ii)(I) approve of the portions of an assessment and emergency response plan submitted pursuant to paragraph (1)(A); or

"(II) disapprove of the portions of an assessment or emergency response plan submitted pursuant to paragraph (1)(A) if the Administrator or the State, as applicable, determines that—

"(aa) the submitted portions of the assessment or emergency response plan are missing, incomplete, or fail to conform with the requirements of this section; or

"(bb) the submitted portions of the assessment or emergency response plan fail to provide for cybersecurity resilience in accordance with the baseline 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

229(b)(2)(A), the Administrator, in consultation with appropriate Federal law enforcement and intelligence officials, shall develop such protocols as are necessary to protect any information provided under paragraph (1)(A) to the State.

''(ii) REQUIREMENTS FOR PROTOCOL.—The protocol developed under clause (i) shall ensure that—

''(I) each copy of the portions of an assessment and emergency response plan submitted pursuant to paragraph (1)(A) are kept in a secure location;

''(II) only individuals designated by the applicable State may have access to copies of the portions of the assessment and emergency response plan submitted pursuant to paragraph (1)(A); and

''(III) no copy of the portions of the assessment and emergency response plan submitted pursuant to paragraph (1)(A) shall be made available to anyone other than an indi-

vidual designated by the applicable State.

''(iii) SAVINGS PROVISION.—Nothing in this subparagraph authorizes any person to withhold any information from Congress or from a committee or subcommittee of Congress.

''(4) APPLICABILITY OF FOIA.—Any findings or plans (including revisions and any related agency records and information that is designated as Department of Defense critical infrastructure security information under section 130e(b) of title 10, United States Code) 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.

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

vising an assessment or emergency response plan under this section.

''(f) RECORD MAINTENANCE.—Each covered treatment works shall maintain a copy of the assessment conducted under subsection (b) and the emergency response plan prepared under subsection (c) (including any revised assessment or plan) for 5 years after the date on which that assessment or plan is approved by the applicable State under this section.

''(g) GUIDANCE TO SMALL TREATMENT WORKS.—The Administrator shall provide guidance and technical assistance to treatment works that are not covered treatment works on how to conduct resilience assessments, prepare emergency response plans, and address threats from malevolent acts and natural hazards that threaten to disrupt the collection, storage, treatment, recycling, and reclamation of municipal sewage or industrial wastes or significantly affect the public health.''.

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

SEC. 202. CYBERSECURITY REQUIREMENTS FOR TREATMENT WORKS.

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

"SEC. 229. CYBERSECURITY REQUIREMENTS.

"(a) DEFINITIONS.—In this section:

"(1) COVERED TREATMENT WORKS.—The term 'covered treatment works' has the meaning given the term in section 228(a).

"(2) 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 cybersecurity resilience of a treatment works.

"(3) CYBERSECURITY RESILIENCE.—The term 'cybersecurity resilience' means the ability of a treatment works to adapt to or withstand the effects of a cybersecurity incident without interruption to the treatment works's function, or if the function is interrupted, to rapidly return to a normal operating condition.

"(4) STATE.—

"(A) IN GENERAL.—Except for subsection (e), the term 'State' means a State that has assumed primary enforcement responsibility pursuant to subsection (e).

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

"(b) CYBERSECURITY ASSESSMENTS.—

"(1) ASSESSMENTS REQUIRED.—

"(A) IN GENERAL.—A State shall carry out cybersecurity assessments of a covered treatment works in accordance with this paragraph.

"(B) EVALUATION OF ADEQUACY.—For a covered treatment works subject to a cybersecurity assessment under subparagraph (A), if the covered treatment works uses operational technology, the State shall evaluate the adequacy of the cybersecurity of the operational technology, and information and communications technology 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-

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

''(3) SUBMISSION TO EPA.—

''(A) IN GENERAL.—A State shall annually submit to the Administrator a report that summarizes the performance of the covered treatment works of the State for each cybersecurity performance metric established by the Administrator under subsection (d)(1) based on the review by the State of risk and resilience assessments pursuant to paragraph (1)(C).

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

''(4) TECHNICAL ASSISTANCE.—The Administrator shall, on request of a covered treatment works, provide guidance and technical assistance to the covered treatment works with respect to—

''(A) implementing any requirement under this section or section 228; and

''(B) enhancing cybersecurity resilience.

''(c) BASELINE CYBERSECURITY STANDARDS.—

''(1) IN GENERAL.—The Administrator shall by rulemaking establish baseline cybersecurity standards that shall serve as requirements to provide for the cybersecurity resilience of a covered treatment works.

''(2) REQUIREMENTS.—In developing and establishing the baseline cybersecurity standards under paragraph (1), the Administrator shall, at a minimum—

''(A) work in conjunction with the Director of the Cybersecurity and Infrastructure Security Agency and the Director of the National Institute of Standards and Technology;

''(B) develop the baseline cybersecurity standards in collaboration with covered treatment works of various sizes and capacities to ensure that feedback from a variety of covered treatment works is considered during the development of the baseline cybersecurity standards;

''(C) ensure that best practices and guidelines that already exist in the water sector at 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) representative from an information technology or operational technology service provider that provides cybersecurity services to covered treatment works; 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 cybersecurity standards account for the varied capacity and risk of all covered treatment works; and

"(B) may establish different baseline cybersecurity standards for different categories of treatment works 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 performance metrics (referred to in this subsection as the 'cybersecurity performance metrics') to be used by the Administrator to measure or assess how well the sector of treatment works in the United States is making progress on implementing cybersecurity best practices.

"(B) ASSESSMENT; REPORT.—The Administrator shall, not less frequently than once every 4 years—

"(i) assess the sector of treatment works in the United States using the cybersecurity performance metrics; and

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

"(2) PROVISION OF INFORMATION.—Notwithstanding any other provision of law, a treatment works may, at the discretion of the treatment works and for the purpose of developing sector-wide risk assessments and performance metrics to measure how treatment works are making progress in developing and implementing cybersecurity best practices, provide to the Administrator, and the Administrator may accept, information that would assist the Administrator in the development and maintenance of the cybersecurity performance metrics.

"(e) ENFORCEMENT; STATE ASSUMPTION OF DUTIES.—

"(1) IN GENERAL.—This section and section 228 shall be enforced by the Administrator unless a State assumes primary enforcement responsibility pursuant to this subsection.

"(2) APPLICATION.—A State seeking to assume primary enforcement responsibility pursuant to this

subsection shall submit to the Administrator an application at such time, in such manner, and containing such information as the Administrator may by regulation require.

''(3) DETERMINATION.—On receiving an application described in paragraph (2) from a State, the Administrator shall, based on that application, determine whether the State—

''(A) has adopted and is implementing adequate procedures for the enforcement of requirements that are no less stringent than those under this section and section 228;

''(B) has adopted authority and has sufficient capacity to impose enforcement remedies in line with those prescribed under this title;

''(C) has sufficient capacity and personnel with sufficient expertise to perform cybersecurity assessments and conduct reviews of risk and resilience assessments and emergency response plans under section 228; and

''(D) has sufficient security mechanisms in place to prevent any unsanctioned disclosure or dissemination of risk and resilience assessments, emergency response plans, and any other information provided by a covered treat-

ment works, in alignment with the protocols developed by the Administrator under section 228(d)(3)(B)(i).

''(4) TIMELINE.—Not later than 180 days after the date on which the Administrator receives an application described in paragraph (2), the Administrator shall—

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

''(B) if the Administrator determines that the State fails to meet 1 or more of the requirements described in paragraph (3), deny the application.

''(5) REVOCATION OF PRIMARY ENFORCEMENT RESPONSIBILITY.—The Administrator may, as appropriate, revoke an assumption of primary enforcement responsibility pursuant to this subsection if the Administrator determines that a State no longer meets 1 or more requirements described in paragraph (3).

''(6) REGULATIONS REQUIRED.—The Administrator shall promulgate regulations carrying out this subsection not later than 1 year after the date of enactment of this section, which shall include—

"(A) the requirements for an application described in paragraph (2);

"(B) the period for which a State may assume primary enforcement responsibility pursuant to this subsection before renewal; and

"(C) the manner by which the Administrator may revoke primary enforcement responsibility pursuant to paragraph (5).

"(7) SAVINGS PROVISION.—An assumption of primary enforcement responsibility pursuant to this subsection shall be separate from any responsibility otherwise assumed under this Act.".

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

(1) by striking "or (4) carrying" and inserting "(4) carrying"; and

(2) by striking "504 of this Act—" and inserting "504; or (5) carrying out requirements under section 229—"

(c) FEDERAL ENFORCEMENT.—Section 309 of the Federal Water Pollution Control Act (33 U.S.C. 1319) (as amended by section 201(b)) is amended in each of subsections (a), (c), (d), and (g) by inserting "229," before "301," each place it appears.

SEC. 203. CLEAN WATER SECURITY ASSISTANCE.

(a) AUTHORIZATION OF APPROPRIATIONS.—In addition to any amounts authorized to be appropriated under section 607 of the Federal Water Pollution Control Act (33 U.S.C. 1387), there is authorized to be appropriated $300,000,000 for each of fiscal years 2027 through 2032 for the purposes of helping treatment works (as defined in section 212 of that Act (33 U.S.C. 1292)) build cybersecurity resilience (as defined in section 229 of the Federal Water Pollution Control Act) and identifying and mitigating cybersecurity vulnerabilities, including those included in risk and resilience assessments and emergency response plans prepared pursuant to section 228 of that Act.

(b) GUIDANCE.—The Administrator of the Environmental Protection Agency may issue guidance to determine specific criteria for eligible uses of the amounts made available under subsection (a) that further the purposes described in that subsection.

(c) PRIORITIZATION.—In using amounts made available pursuant to subsection (a), a State shall prioritize providing assistance to treatment works (as defined in section 212 of the Federal Water Pollution Control Act (33 U.S.C. 1292)) that have the greatest need with respect to capacity, workforce, expertise, or resources to adequately address cybersecurity vulnerabilities.

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

TITLE III—CYBER INCIDENT REPORTING OBLIGATIONS

SEC. 301. CYBER INCIDENT REPORTING.

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

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

''(4) COVERED ENTITY.—The term 'covered entity'—

''(A) means an entity in a critical infrastructure sector, as defined in Presidential Policy Directive 21, that satisfies the definition established by the Director in the final rule issued pursuant to section 2242(b); and

''(B) includes—

''(i) 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 greater than 3,300 persons; and

"(ii) a covered treatment works (as defined in section 228(a) of the Federal Water Pollution Control Act).";

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

"(8) TRANSMISSION TO EPA.—The Agency shall submit to the Administrator of the Environmental Protection Agency a copy of each report submitted to the Agency under paragraph (1), (2), or (3).";

and

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

(A) by striking "This section" and inserting the following:

"(1) IN GENERAL.—Except as provided in paragraph (2), this section"; and

(B) by adding at the end the following:

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