

## Federal Affairs Committee

May 5, 2026

3:30-5:00pm PT

Ballroom A 4-6, SAFE Credit Union Convention Center

Sacramento, CA

Chair, Jolene Walsh

Vice-Chair, Scott Petersen

---

- I. Welcome & Call to Order, Jolene Walsh, Federal Affairs Committee Chair
- II. Introductions
- III. Approval of January 28, 2026 Meeting Minutes
- IV. Regulatory Update: Caleb Raspler
- V. Federal Update: Ian Lyle
- VI. ACWA Update Vision for Our Water Future: Chelsea Haines
- VII. Samantha Barncastle, Family Farm Alliance
- VIII. Legislative Voting Session: Ian Lyle / Libby Spekhardt
  - a. DROUGHT Act (H.R.7845) – Support (Subcommittee recommendation)
  - b. Water Project Navigators Act (S.3792/H.R.7408) – Support (Subcommittee recommendation)
  - c. Community Water Project Acceleration Act (S.4120) – Favor (Subcommittee recommendation)
  - d. Data Center Water and Energy Transparency Act (S.4213) – Watch (Subcommittee recommendation)
- IX. Legislative discussion: Draft water sector cybersecurity legislation
- X. 2026-27 Committee Work Plan
- XI. Organizational Partner Update: Eric Nagy, National Waterways Conference Board of Directors, NESARC, Family Farm Alliance
- XII. 2026 Upcoming Meeting Dates:
  - a. September 2026
  - b. December 1, 2026 – ACWA Fall Conference – Anaheim, CA

Minutes ACWA  
Federal Affairs Committee  
January 28, 2026  
3:30 Pacific/5:00pm Pacific Time  
Virtual only – Hosted on Zoom

---

### **Meeting Called to Order**

ACWA Federal Affairs Committee Chair Jolene Walsh called the meeting to order at 3:35pm Pacific Time.

### **Approval of Minutes**

Minutes from the Federal Affairs Committee's December 2, 2025, meeting were reviewed and approved by voice vote.

### **Committee Orientation**

Ian Lyle led a committee orientation for the Federal Affairs Committee, covering ACWA's history, governance structure, and the role of the Board in guiding the association's policy priorities. He also reviewed ACWA's Code of Conduct, provided an overview of ACWA's regional structure and committee reporter process, and walked through the composition and governance of ACWA's standing committees.

### **Updates**

Congressional Update – Ian Lyle provided an overview covering some of the recent actions in the House of Representatives and the U.S. Senate. Information included an update on FY2027 appropriations, including a minibus package passing Congress to fund various federal water programs ([H.R.6938](#)), which passed in the House by a 397-28 vote on January 8<sup>th</sup> and passed the Senate by an 82-15 vote on January 15<sup>th</sup>. Mr. Lyle also reported on the U.S. House of Representatives passing the remainder of their appropriations funding bills, completing the FY26 appropriations process in the chamber ([H.R.7148](#)). The bill will head to the Senate next for consideration. ACWA supported FEMA Act passing out of the House T&I Committee as well as an overview of the House passed Energy and Water Appropriations bill. There was also a broader discussion about appropriations and the possibility of a federal government shutdown.

Regulatory Update - Caleb Raspler reported that EPA recently advanced several drinking water and Clean Water Act rulemakings of interest to ACWA members. EPA proposed updates to Clean Water Act Section 401 water quality certification on January 15; while ACWA does not plan to comment, interested members are encouraged to submit comments by February 17. EPA also released a draft National Primary Drinking Water Regulation for perchlorate on January 6, proposing an MCL between 20–80 ppb, which ACWA is reviewing and will coordinate member comments on, and published a Fluoride Preliminary Assessment Plan on January 28 to inform potential revisions to federal fluoride standards, though ACWA does not plan to comment and encourages interested members to do so by February 27.

The Federal Affairs Committee reviewed and adopted positions on 4 bills as noted below:

- S.3738 – MORE WATER Act – Support and amend
- S.3737 – GROW SMART Act - Support

- S.3465 – UPGRADES Act - Favor
- S.3609/H.R.582 - Community Protection Wildfire Resilience Act - Favor

**Other Items:**

Staff discussed ACWA's upcoming DC Conference on February 24 -26, 2026, at the Willard Hotel in Washington, D.C. ACWA staff encouraged committee members to nominate a Federal Affairs Committee member for the Federal Affairs Outreach Award that is announced every DC Conference. The "Most Effective Agency on a Federal Issue" is awarded to an agency that has engaged on a federal issue as prioritized by the ACWA Federal Affairs Committee. The award recipient will be selected based on the total number of federal interactions and with consideration of the importance of the issue. Ian Lyle previewed monthly committee briefings that the Committee will begin holding this year to make voting sessions during more efficient between in-person full committee meetings.

**Upcoming Meetings:** The next meeting of ACWA's Federal Affairs Committee will take place on May 5, 2026, in person at ACWA's Spring Conference in Sacramento, California. A meeting to-be-determined will be held in September. The final meeting of the year will take place on December 1, 2026, at ACWA's Fall Conference in Anaheim, California.

The meeting adjourned at 4:43pm Pacific Time.

## **Attendance ACWA Federal Affairs Committee Meeting**

**January 28, 2026**

### **FAC Committee Members Attendance:**

Brad Sherwood, Sonoma Water, Region 1  
Dennis Mayo, McKinleyville Community Services District, Region 1  
Nicole Dorotinsky, City of Santa Rosa – Water Department, Region 1  
Adam Robin, Yuba Water Agency, Region 2  
Ernest Conant, Tehama-Colusa Canal Authority, Region 2  
Kevin Phillips, Paradise Irrigation District, Region 2  
Chris Wilson, Placer County Water Agency, Region 3  
Glen Jacobs, Tuolumne Utilities District, Region 3  
Nicholas Schneider, Georgetown Divide Public Utility District, Region 3  
Sarah Starr, City of Roseville, Region 3  
Anne Sanger, City of Sacramento – Department of Utilities, Region 4  
Dana Ferreira, Modesto Irrigation District, Region 4  
Greg Zlotnick, San Juan Water District, Region 4  
Josh Weimer, Turlock Irrigation District, Region 4  
Katie Patterson, South San Joaquin Irrigation District, Region 4  
Andrew DeGraca, San Francisco Public Utilities Commission, Region 5  
Beckie Zisser, Valley Water, Region 5  
John Weed, Alameda County Water District, Region 5  
Mauricio Guardado, United Water Conservation District, Region 5  
Rachel Murphy, Contra Costa Water District, Region 5  
Brandy Swisher, Kings River Conservation District, Region 6  
Cristel Tufenkjian, McMullin Area Groundwater Sustainability Agency, Region 6  
G. Patrick O'Dowd, Dudley Ridge Water District, Region 6  
Brett Stroud, Wheeler Ridge-Maricopa Water Storage District, Region 7  
Craig Wallace, Kern County Water Agency, Region 7  
Johnny Amaral, Friant Water Authority, Region 7  
Kris Lawrence, Shafter-Wasco Irrigation District, Region 7  
Abby Schneider, Metropolitan Water District of Southern California, Region 8  
Anthony Fellow, Upper San Gabriel Valley MWD, Region 8  
Jason Maruca, City of Burbank – Water and Power, Region 8  
Matthew Veeh, West Basin Municipal Water District, Region 8  
Terrence McCarthy, Los Angeles Department of Water & Power, Region 8  
Arman Tarzi, Jurupa Community Services District, Region 9  
Colby Lawton, Rancho Water, Region 9  
Marion Champion, Mission Springs Water District, Region 9  
Michael Hadley, Western Municipal Water District, Region 9  
Alexandra Berenter, City of San Diego – Public Utilities, Region 10  
Cathy Green, Orange County Water District, Region 10  
Kyle Swanson, Padre Dam Municipal Water District, Region 10  
Mark Toy, Yorba Linda Water District, Region 10

### **Federal Affairs Committee Excused Absences:**

Jeffrey Sutton, Glenn-Colusa Irrigation District, Region 2  
Scott Ratterman, Calaveras County Water District, Region 3  
Harvey Ryan, Elsinore Valley Municipal Water District, Region 9  
Kathleen Hedberg, Helix Water District, Region 10

**Drought Relief Obtained Using Government Help Today (DROUGHT) Act  
(H.R.7845)**

On March 5, 2026, Congressman Scott Peters (D-CA-50) introduced H.R.7845, the Drought Relief Obtained Using Government Help Today (DROUGHT) Act. Original cosponsors of the bill include Reps. Sara Jacobs (CA-51), Jim Costa (CA-21), Mike Levin (CA-49), Juan Vargas (CA-52), John Garamendi (CA-8), and Nanette Barragán (CA-44).

The DROUGHT Act would increase the EPA WIFIA program's federal funding assistance cap to ninety percent for water infrastructure projects with regional or national significance, projects in drought-stricken areas, or projects in low-income communities.

Currently, under the Water Infrastructure Finance and Innovation Act (WIFIA), federal loans under the WIFIA program can only cover up to eighty percent of water infrastructure project costs. Increasing the program's federal assistance threshold will provide financial relief for critical water infrastructure projects and reduce barriers to receiving low-interest loans in the interest of providing safe drinking water for communities.

The DROUGHT Act has been referred to the House Committee on Transportation and Infrastructure and the Committee on Energy and Commerce. Congressman Huffman and Senator Padilla submitted the DROUGHT Act for inclusion in the 2026 Water Resources Development Act (WRDA).

**Subcommittee Recommendation: Support**

**Water Project Navigators Act (S.3792/H.R.7408)**

On February 5, 2026, Senators John Hickenlooper (D-CO) and Jerry Moran (R-KS) introduced the Water Project Navigators Act (S.3792). U.S. Representatives Brittany Petersen (D-CO-07) and Juan Ciscomani (R-AZ-06) introduced an identical bill in the House (H.R.7408).

The Water Project Navigators Act would authorize a grant program at the Department of the Interior within the Bureau of Reclamation to provide funding to States, tribes, disadvantaged and rural communities, and other eligible entities to support multi-benefit water project navigator positions. These positions would provide services such as technical assistance in the support of The Water Project Navigators Program would provide three-year grants for navigators to assist multi-benefit water project projects that address drought and ecosystem resilience and water efficiency while providing benefits to watersheds and ecosystems.

The bill authorizes \$90 million over six years (FY2027 – FY2032) for the Water Project Navigators Program and offers a federal cost share of up to 75 percent with the opportunity to extend the grant contract for up to two years with additional funding included. Additionally, Reclamation would have authority to waive the non-Federal cost share of the project if that share is proven to result in financial hardship for the grant recipient.

The Water Project Navigators Act has been referred to the Senate Committee on Energy and Natural Resources and the House Committee on Natural Resources. The Senate ENR Water and Power Subcommittee held a legislative hearing on the bill on March 17, 2026.

**Subcommittee Recommendation: Support**

## **Community Water Project Acceleration Act (S.4120)**

On March 17, 2026, Senator Mark Kelly (D-AZ) introduced S.4120, the Community Water Project Acceleration Act. Cosponsored by Senator Cynthia Lummis (R-WY), the Community Water Project Acceleration Act seeks to designate categorical exclusions from certain National Environmental Policy Act (NEPA) requirements for Army Corps Civil Works projects when:

1. The federal contribution to the project is less than \$6 million; **or**
2. Federal funding makes up less than 15 percent of the total project cost

The concept of the bill mirrors an authorized pathway for categorical exclusions for federal transportation projects with limited federal assistance included in Sec 1317 of [MAP-21](#) - a two-year transportation reauthorization bill passed during the Obama administration in 2012.

Streamlining environmental reviews for critical water infrastructure projects will reduce delays in construction and increased costs for water utilities and local project sponsors. ACWA supports the responsible streamlining of environmental reviews to ensure that water utilities are receiving federal funding in a timely manner to deliver a safe and reliable water supply.

The Community Water Project Acceleration Act has been referred to the Senate Committee on Environment and Public Works.

**Subcommittee Recommendation:** Favor

### **Data Center Water and Energy Transparency Act (S.4213)**

On March 25, 2026, U.S. Senator Dick Durbin (D-IL) introduced the Data Center Water and Energy Transparency Act (S.4213). It would require qualifying data centers to submit annual reports to states (or to EPA, USDA, or DOE if a state does not establish a reporting program).

ACWA recognizes the growth in demand for data centers across the country and in California and the nexus between data centers and water. Data center development, like any industry, is represented by a spectrum of entities ranging from large companies like Microsoft and Amazon to small businesses. Recent media coverage has heightened interest in tracking energy and water use associated with Data Center development, and in some instances the lack of data. Several members of Congress have approached ACWA staff with questions regarding water and data center development.

ACWA has not taken a formal position on general data center development at the federal level, but has encouraged information sharing and recognizes the importance of water to data centers. Last year, ACWA filed several sets of comments to this effect as part of the National AI Strategic Plan and recently partnered with the National Waterways Conference, the Western States Water Council, the Interstate Council on Water Policy, and the Texas Water Association in an effort to facilitate conversations and information sharing between water providers and data center developers. ACWA also welcomes the study and adoption of innovative water efficiency methods to keep up with the large overhead costs of data center water use for evaporative cooling systems.

The Data Center Water and Energy Transparency Act referred to the Committee on Energy and Natural Resources.

**Subcommittee Recommendation:** Watch

## **Draft water sector cybersecurity legislation (S. \_\_\_\_)**

Senator Schiff's team has requested feedback from ACWA on a draft cybersecurity bill. The legislation would amend the Safe Drinking Water Act and the Federal Water Pollution Control Act to establish cybersecurity requirements for both drinking water and wastewater systems.

### **Title I: Drinking water requirements:**

The Safe Drinking Water Act currently requires drinking water providers to conduct risk and resilience assessments every five years and to develop emergency response plans to help address identified risks. Under current law cyber security considerations are not a required part of the assessment. The bill amends the Safe Drinking Water Act to require cybersecurity threats be included in drinking water utilities risk and resilience assessments and cybersecurity counter measures be added to the emergency response plan. Maintains the requirement for assessments to be done every five years.

Smaller providers, those serving less than 3,300 would be exempt from these requirements.

### **Title II: Wastewater requirements:**

Wastewater systems are not currently required to conduct risk and resilience assessments. However, many do in accordance with EPA and industry guidance. Senator Schiff's legislation would make risk and resilience assessments and emergency response plans mandatory for wastewater treatment works and include a requirement to consider cybersecurity threats and countermeasures.

A covered treatment work is defined as serving 10,000 persons and has a design flow rate of 1,000,000 gallons or more.

### **EPA Reporting (both drinking and wastewater):**

The bill directs EPA to establish cybersecurity performance metrics to measure progress of public drinking water systems and wastewater systems in implementing cybersecurity best practices. When developing performance metrics EPA is directed to work with the Cybersecurity and Infrastructure Security Agency (CISA). EPA is also required to consult public water agencies when developing the requirements. Reporting would be exempt from FOIA.

### **Considerations:**

Under this legislation cybersecurity practices for the public drinking water and wastewater sector would shift from voluntary to mandatory.

Enforcement would be carried out under existing authorities of the Safe Drinking Water Act which can include fines (up to over \$70,000 per day per violation).

Funding- the bill authorizes significant funding to help address cybersecurity issues. A total of \$3.5 billion broken down as follows:

- For Drinking Water Providers:
  - \$250 million (50 million annually FY 27-32) via a reauthorization of the Drinking Water Infrastructure Risk and Resilience Program (prior auth was 25 million annually)
  - \$1.5 billion (300 million annually FY-27-32) for identifying and mitigating cybersecurity vulnerabilities
- For Wastewater:
  - \$250 million (50 million annually FY27-32) via a reauthorization to the Clean Water Infrastructure Resiliency and Sustainability Program (prior auth was \$25 million).
  - \$1.5 billion (\$300 million annually FY27-32) for identifying and mitigation cybersecurity vulnerabilities in treatment works.

**Staff Recommendation:** The bill is in draft form and Senator Schiff's team has been receptive to early ACWA feedback on the legislation. As of today, there is not a set date for introduction of the bill, but his team has indicated they would like to introduce it this summer. We would like to get feedback from ACWA members about their thoughts on the bill and any potential changes they would like to see made to the bill with the goal of getting ACWA to a favor or support position for the legislation.

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.

Mr. Schiff introduced the following bill; which was read twice and referred to the Committee on \_\_\_\_\_

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 [“\_\_\_\_\_ Act of \_\_\_\_”].

(b) Table of Contents.—The table of contents for 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.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.

## 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 of by the Administrator or the applicable State and subject to paragraph (4), if the State has assumed primary enforcement responsibility pursuant to section 1433A(c), 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 the assessment that the system conducted under that paragraph to determine if the assessment should be revised.

“(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 Administrator or the applicable State, if the State has assumed primary enforcement responsibility pursuant to section 1433A(c), a certification that the community water system has reviewed and, if applicable, revised the assessment.

“(4) REQUIREMENT.—Each method approved of by the Administrator or a State under paragraph (1)(A)(vii) shall include an evaluation of each cybersecurity performance metric established by the Administrator under section 1433A(b)(1).”;

(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 (and 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 (and, except as provided in paragraph (3), take no longer than 2 years 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) GREATER NEED SYSTEMS.—The Administrator may extend the 2-year period described in paragraph (2)(E) for an additional year for such categories of community water systems as the Administrator determines have greater need.

“(4) 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(a)(2)(A), provide to the Administrator or the applicable State, if that State has assumed primary enforcement responsibility pursuant to section 1433A(c), the assessments of the community water system under subsection (a) and the emergency response plans prepared under subsection (b) (including any revised assessment or plan).

“(B) TREATMENT OF INFORMATION.—Any information included in a document provided under subparagraph (A) that is designated as Department of Defense critical infrastructure security information under subsection (b) of section 130e of title 10, United States Code, or is similar to such information, shall be provided in a manner that is protective of national security consistent with that section.

“(2) REVIEW; APPROVAL.—

“(A) IN GENERAL.—The Administrator, in consultation with the applicable State, or the State, if the State has assumed primary enforcement responsibility pursuant to section 1433A(c), shall—

“(i) review the assessments and emergency response plans submitted under paragraph (1) for conformity with the requirements of this section and section 1433A; and

“(ii)(I) approve of the assessments and emergency response plan of a

community water system; or

“(II) disapprove of the assessments or emergency response plan of a community water system if the Administrator or State, as applicable, determines that—

“(aa) the assessments or emergency response plan is missing, incomplete, or fails to conform with the requirements of this section or section 1433A; or

“(bb) the emergency response plan fails to mitigate a significant cybersecurity risk, as identified under subsection (a)(1)(A)(vii).

“(B) ENFORCEMENT.—The Administrator or the State, if the State has assumed primary enforcement responsibility pursuant to section 1433A(c), may, in the determination of the Administrator or the State, as applicable, use appropriate enforcement mechanisms under this title to remedy noncompliance under this subsection.

“(3) SUBMITTED DOCUMENTATION.—

“(A) 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.

“(B) TREATMENT OF DOCUMENTATION.—The Administrator, or a State that has assumed primary enforcement responsibility pursuant to section 1433A(c), shall ensure that the documentation described in subparagraph (A) remains secure and protected from any disclosure or dissemination that could increase the risk of harm to a public water system or a community served by a public water system.”;

(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 Administrator or a State, if the State has assumed primary enforcement responsibility pursuant to section 1433A(c),”; and

(7) in subsection (g)(6), by striking “\$25,000,000 for each of fiscal years 2020 and 2021” and inserting “\$50,000,000 for each of fiscal years 2027 through 2032”.

## 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) Cybersecurity Assessments.—

1 “(1) DEFINITION OF SIGNIFICANT CYBERSECURITY DEFICIENCY.—In this subsection, the  
2 term ‘significant cybersecurity deficiency’ means the absence of a practice or control, or the  
3 presence of a vulnerability, that could compromise operational technology and, as a result,  
4 cause a potential impact described in subparagraph (A) or (B) of section 1433(a)(2).

5 “(2) ASSESSMENTS REQUIRED.—

6 “(A) IN GENERAL.—The Administrator or the State, if the State has assumed primary  
7 enforcement responsibility pursuant to subsection (c), shall carry out cybersecurity  
8 assessments, including through inspections, of the systems of a public water system in  
9 accordance with this paragraph.

10 “(B) EVALUATION OF ADEQUACY.—For a public water system subject to a  
11 cybersecurity assessment under subparagraph (A), the Administrator or the State, as  
12 applicable, shall evaluate the adequacy of the cybersecurity of the operational  
13 technology for producing and distributing safe drinking water.

14 “(C) REVIEW OF ASSESSMENTS AND PLANS.—In carrying out a cybersecurity  
15 assessment required under subparagraph (A), a public water system shall provide, and  
16 the Administrator or the State, as applicable, shall review, the risk and resilience  
17 assessments of the public water system under section 1433(a) and the emergency  
18 response plans of the public water system under section 1433(b).

19 “(3) SIGNIFICANT CYBERSECURITY DEFICIENCIES.—If the Administrator or the State, as  
20 applicable, identifies a significant cybersecurity deficiency, the Administrator or the State,  
21 as applicable, shall take appropriate steps to address the significant cybersecurity deficiency  
22 and use mechanisms, including enforcement, for failures to correct those significant  
23 cybersecurity deficiencies.

24 “(4) SUBMISSION TO EPA.—A State that has assumed primary enforcement responsibility  
25 pursuant to subsection (c) shall annually submit to the Administrator a report that  
26 summarizes the performance of the public water systems of the State for each cybersecurity  
27 performance metric established by the Administrator under subsection (b)(1) based on the  
28 review by the State of risk and resilience assessments pursuant to paragraph (2)(C).

29 “(5) TECHNICAL ASSISTANCE.—The Administrator shall, on request of a public water  
30 system, provide guidance and technical assistance to the public water system with respect  
31 to—

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

33 “(B) addressing significant cybersecurity vulnerabilities.

34 “(b) Sharing of Information for Cybersecurity Performance Metrics.—

35 “(1) ESTABLISHMENT OF CYBERSECURITY PERFORMANCE METRICS.—

36 “(A) IN GENERAL.—Not later than 2 years after the date of enactment of this section,  
37 the Administrator shall establish cybersecurity performance metrics (referred to in this  
38 subsection as the ‘cybersecurity performance metrics’) to be used by the Administrator  
39 to measure or assess cybersecurity-related activities, incidents, and the progress of  
40 efforts by public water systems to enhance cybersecurity protections and to determine  
41 how well the sector is making progress on implementing cybersecurity best practices.

1 “(B) REQUIREMENTS.—In developing and establishing the cybersecurity  
2 performance metrics, the Administrator shall, at a minimum—

3 “(i) work in conjunction with the Director of the Cybersecurity and  
4 Infrastructure Security Agency;

5 “(ii) consult with public water systems of various sizes and capacities to ensure  
6 that feedback from a variety of public water systems is considered during the  
7 development of the cybersecurity performance metrics; and

8 “(iii) consider—

9 “(I) the feedback and concerns obtained in the consultations required  
10 under clause (ii);

11 “(II) the time to correct a significant cybersecurity risk after identification  
12 under section 1433(a)(1)(A)(vii) or a cybersecurity significant deficiency  
13 after identification under subsection (a)(3);

14 “(III) backup or recovery capacity in the event that an information system  
15 or significant physical component of an operational technology system of a  
16 public water system is rendered inoperable;

17 “(IV) the number of public water systems that have a dedicated  
18 cybersecurity lead or cybersecurity team, either through direct hiring of staff  
19 or entering into contracts for such services;

20 “(V) the number of public water systems that update risk and resilience  
21 assessments every 5 years, as required under section 1433(a)(4);

22 “(VI) the number of community water systems serving a population of  
23 greater than 3,300 persons that are in compliance with section 1433;

24 “(VII) the time to restore the functionality of a public water system or an  
25 information system or significant physical component of an operational  
26 technology system of a public water system that was rendered inoperable by  
27 an incident; and

28 “(VIII) the percentage increase or decrease in incidents that affect public  
29 water systems over time.

30 “(C) ASSESSMENT; REPORT.—The Administrator shall annually—

31 “(i) assess public water systems using the cybersecurity performance metrics;  
32 and

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

36 “(2) PROVISION OF INFORMATION.—Notwithstanding any other provision of law, a public  
37 water system may, at the discretion of the public water system and for the purpose of  
38 developing sector-wide risk assessments and performance metrics to measure how public  
39 water systems are making progress in developing and implementing cybersecurity best  
40 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.

“(c) 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 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 disclosure or dissemination of risk and resilience assessments, emergency response plans, and any other information provided by a public water system that could increase the risk of harm to the public water system or a community served by the public water system.

“(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) 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 identifying and mitigating cybersecurity vulnerabilities in public water systems (as defined in section 1401 of that Act (42 U.S.C. 300f)), 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.

1 “(3) RESILIENCE.—The term ‘resilience’ means the ability of a treatment works or an  
2 asset of a treatment works to adapt to, or withstand the effects of, a malevolent act or  
3 natural hazard without interruption to the function of the treatment works or asset or, if the  
4 function is interrupted, to rapidly return to a normal operating condition.

5 “(b) Risk and Resilience Assessments.—

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

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

9 “(A) shall include an assessment of—

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

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

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

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

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

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

20 “(vii) using a method approved by the Administrator or the applicable State and  
21 subject to paragraph (5), if the State has assumed primary enforcement  
22 responsibility pursuant to section 229(d), the risks to electronic, computer, or  
23 other automated systems for the purpose of identifying significant cybersecurity  
24 risks that have the potential to cause the impacts described in subparagraph (A) or  
25 (B) of paragraph (3); and

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

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

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

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

38 “(4) REVIEW AND REVISION.—

39 “(A) IN GENERAL.—Each covered treatment works shall, not less frequently than

once every 5 years, review the assessment that the covered treatment works conducted under paragraph (1) to determine if the assessment should be revised.

“(B) CERTIFICATION TO THE ADMINISTRATOR OR STATE.—On completion of the review under subparagraph (A), a covered treatment works shall submit to the Administrator or the applicable State, if the State has assumed primary enforcement responsibility pursuant to section 229(d), a certification that the covered treatment works has reviewed and, if applicable, revised the assessment.

“(5) REQUIREMENT.—Each method approved of by the Administrator or a State under paragraph (2)(A)(vii) shall include an evaluation of each cybersecurity metric established by the Administrator under section 229(c)(1).

“(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 impact 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 (and, except as provided in paragraph (3), take no longer than 2 years 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) GREATER NEED SYSTEMS.—The Administrator may extend the 2-year period described in paragraph (2)(E) for an additional year for such categories of covered treatment works as the Administrator determines have greater need.

“(4) 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 “(1) SUBMISSION.—

2 “(A) IN GENERAL.—Beginning not later than 1 year after the date on which the  
3 Administrator provides baseline information under subsection (b)(3), each covered  
4 treatment works shall, during a cybersecurity assessment pursuant to section  
5 229(b)(2)(A), provide to the Administrator or the applicable State, if the State has  
6 assumed primary enforcement responsibility pursuant to section 229(d), any  
7 assessments under subsection (b) and the emergency response plans prepared under  
8 subsection (c) (including any revised assessment or plan).

9 “(B) TREATMENT OF INFORMATION.—Any information included in a document  
10 provided under subparagraph (A) that is designated as Department of Defense critical  
11 infrastructure security information under subsection (b) of section 130e of title 10,  
12 United States Code, or is similar to such information, shall be provided in a manner  
13 that is protective of national security consistent with that section.

14 “(2) REVIEW; APPROVAL.—

15 “(A) IN GENERAL.—The Administrator, in consultation with the applicable State, or  
16 the State, if the State has assumed primary enforcement responsibility pursuant to  
17 section 229(d), shall—

18 “(i) review the assessments and emergency response plans submitted under  
19 paragraph (1) for conformity with the requirements of this section and section  
20 229; and

21 “(ii)(I) approve of the assessments and emergency response plan of a covered  
22 treatment works; or

23 “(II) disapprove of the assessments or emergency response plan of a covered  
24 treatment works if the Administrator or the State, as applicable, determines that—

25 “(aa) the assessments or emergency response plan is missing, incomplete,  
26 or fails to conform with the requirements of this section; or

27 “(bb) the emergency response plan fails to mitigate a significant  
28 cybersecurity risk, as identified under subsection (b)(2)(A)(vii).

29 “(B) ENFORCEMENT.—The Administrator or the State, if the State has assumed  
30 primary enforcement responsibility pursuant to section 229(d), may, in the  
31 determination of the Administrator or the State, as applicable, use appropriate  
32 enforcement mechanisms under this Act to remedy noncompliance under this  
33 subsection.

34 “(3) SUBMITTED DOCUMENTATION.—

35 “(A) APPLICABILITY OF FOIA.—Any findings or plans (including revisions and any  
36 related agency records and information that is designated as Department of Defense  
37 critical infrastructure security information under section 130e(b) of title 10, United  
38 States Code) submitted under this subsection shall be exempt from disclosure under  
39 section 552(b)(3) of title 5, United States Code (commonly known as the ‘Freedom of  
40 Information Act’), and any provision of State, Tribal, or local freedom of information  
41 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.—The Administrator, or a State that has assumed primary enforcement responsibility pursuant to section 229(d), shall ensure that the documentation described in subparagraph (A) remains secure and protected from any disclosure or dissemination that could increase the risk of harm to a covered treatment works or a community served by a covered treatment works.

“(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 revising 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 Administrator or State, if the State has assumed primary enforcement responsibility pursuant to section 229(d), 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.

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

## “SEC. 229. CYBERSECURITY REQUIREMENTS.

“(a) Definition of Covered Treatment Works.—In this section, the term ‘covered treatment works’ has the meaning given the term in section 228(a).

“(b) Cybersecurity Assessments.—

“(1) DEFINITION OF SIGNIFICANT CYBERSECURITY DEFICIENCY.—In this subsection, the

term ‘significant cybersecurity deficiency’ means the absence of a practice or control, or the presence of a vulnerability, that could compromise operational technology used in the storage, treatment, recycling, and reclamation of municipal sewage or industrial wastes and, as a result, cause a potential impact described in subparagraph (A) or (B) of section 228(b)(3).

“(2) ASSESSMENTS REQUIRED.—

“(A) IN GENERAL.—The Administrator or the State, if the State has assumed primary enforcement responsibility pursuant to subsection (d), shall carry out cybersecurity assessments, including through inspections, of the systems 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), the Administrator or the State, as applicable, shall evaluate the adequacy of the cybersecurity of the operational technology for maintaining compliance with effluent limitations and preventing the unauthorized discharge of pollutants into the waters of the United States.

“(C) REVIEW OF ASSESSMENTS AND PLANS.—In carrying out a cybersecurity assessment required under subparagraph (A), a covered treatment works shall provide, and the Administrator or the State, as applicable, shall review, the risk and resilience assessments of the public water system under section 228(b) and the emergency response plans of the public water system under section 228(c).

“(3) SIGNIFICANT CYBERSECURITY DEFICIENCIES.—If the Administrator or the State, as applicable, identifies a significant cybersecurity deficiency, the Administrator or the State, as applicable, shall take appropriate steps to address the significant cybersecurity deficiency and use mechanisms, including enforcement, for failures to correct those significant cybersecurity deficiencies.

“(4) SUBMISSION TO EPA.—A State that has assumed primary enforcement responsibility pursuant to subsection (d) 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 (c)(1) based on the review by the State of risk and resilience assessments pursuant to paragraph (2)(C).

“(5) 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) addressing significant cybersecurity vulnerabilities.

“(c) Sharing of Information for Cybersecurity Performance Metrics.—

“(1) ESTABLISHMENT OF CYBERSECURITY PERFORMANCE 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

1 to measure or assess cybersecurity-related activities, incidents, and the progress of  
2 efforts by treatment works to enhance cybersecurity protections and to determine how  
3 well the sector is making progress on implementing cybersecurity best practices.

4 “(B) REQUIREMENTS.—In developing and establishing the cybersecurity  
5 performance metrics, the Administrator shall, at a minimum—

6 “(i) work in conjunction with the Director of the Cybersecurity and  
7 Infrastructure Security Agency;

8 “(ii) consult with treatment works of various sizes and capacities to ensure that  
9 feedback from a variety of treatment works is considered during the development  
10 of the cybersecurity performance metrics; and

11 “(iii) consider—

12 “(I) the feedback and concerns obtained in the consultations required  
13 under clause (ii);

14 “(II) the time to correct a significant cybersecurity risk after identification  
15 under section 228(b)(2)(A)(vii) or to correct a significant cybersecurity  
16 deficiency after identification under subsection (b)(3);

17 “(III) backup or recovery capacity in the event that an information system  
18 or significant physical component of an operational technology system of a  
19 treatment works is rendered inoperable;

20 “(IV) the number of treatment works that have a dedicated cybersecurity  
21 lead or cybersecurity team, either through direct hiring of staff or entering  
22 into contracts for such services;

23 “(V) the number of treatment works that update risk and resilience  
24 assessments every 5 years, as required under section 228(b)(4);

25 “(VI) the number of covered treatment works that are in compliance with  
26 section 228;

27 “(VII) the time to restore the functionality of a treatment works or an  
28 information system or significant physical component of an operational  
29 technology system of a treatment works that was rendered inoperable by an  
30 incident; and

31 “(VIII) the percentage increase or decrease in incidents that affect  
32 treatment works over time.

33 “(C) ASSESSMENT; REPORT.—The Administrator shall annually—

34 “(i) assess treatment works using the cybersecurity performance metrics; and

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

38 “(2) PROVISION OF INFORMATION.—Notwithstanding any other provision of law, a  
39 treatment works may, at the discretion of the treatment works and for the purpose of  
40 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.

“(d) 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 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 disclosure or dissemination of risk and resilience assessments, emergency response plans, and any other information provided by a covered treatment works that could increase the risk of harm to the covered treatment works or a community served by the covered treatment works.

“(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.”.

## SEC. 203. REAUTHORIZATION OF THE CLEAN WATER INFRASTRUCTURE RESILIENCY AND SUSTAINABILITY PROGRAM.

Section 223 of the Federal Water Pollution Control Act (33 U.S.C. 1302a) is amended—

(1) in subsection (c)(5), by inserting “or to assist in the planning, design, construction, or implementation of a program or project consistent with an emergency response plan prepared pursuant to section 228(c)” after “as applicable”; and

(2) in subsection (g)(1), by striking “\$25,000,000 for each of fiscal years 2022 through 2026” and inserting “\$50,000,000 for each of fiscal years 2027 through 2032”.

## SEC. 204. 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 identifying and mitigating cybersecurity vulnerabilities in treatment works (as defined in section 212 of that Act (33 U.S.C. 1292)), 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.

Section 2240 of the Homeland Security Act of 2002 (6 U.S.C. 681) is amended 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).”.