

A REPORT BY
THE 2019-2020 CONTRA COSTA COUNTY CIVIL GRAND JURY
725 Court Street
Martinez, California 94553

Report 2002

Securing Our Water Supply From Cyberattack

APPROVED BY THE GRAND JURY

Date 4/23/2020


ANNE N. GRANLUND
GRAND JURY FOREPERSON

ACCEPTED FOR FILING

Date APR 23 2020


ANITA SANTOS
JUDGE OF THE SUPERIOR COURT

Contra Costa County Civil Grand Jury Report 2002

Securing Our Water Supply From Cyberattack

**TO: Board of Directors, Contra Costa Water District,
Board of Directors, East Bay Municipal Utilities District**

SUMMARY

Contra Costa County residents rely on the water districts to deliver safe, clean water for drinking, cleaning, and sanitation. The government sets standards for water purity, and the water districts must abide by the standards.

Terrorist attacks – both foreign and domestic – are on the rise around the world. Terrorism is the unlawful use of force and violence against a government or agency in furtherance of political or social objectives. The disruption of society through the destruction of our infrastructure is one form of these attacks. Water is a crucial infrastructure, with two primary agencies providing water to Contra Costa County residents – Contra Costa Water District and East Bay Municipal Utilities District. This investigation focuses on these two agencies and asks the following questions:

- Is Contra Costa's water supply safe from a cyberattack (also called a computer attack)?
- Are Contra Costa's primary water districts taking all required measures to secure the water supply?
- Are the water districts informing the public and their customers about the measures they are taking to keep the public water supply safe?

The Grand Jury concluded both districts have plans in place to protect Contra Costa's water supply from cyberattacks and meet the new federal requirements for assessing, certifying, and developing an emergency response plan required by August 31, 2020.

The Grand Jury recommends the water districts consider using the guidance provided by the United States Environmental Protection Agency to meet the requirements of the

American Water Infrastructure Act. The Grand Jury recommends the water districts consider updating their security policy statements and publish the statements on their public websites. Finally, the Grand Jury recommends the water districts consider applying for grants under the federal Drinking Water Infrastructure Risk and Resilience Program to strengthen the resilience of their water systems and offset costs that might otherwise be paid by customers.

METHODOLOGY

The Grand Jury used the following investigative methods:

- Interviewed Contra Costa Water District (CCWD) and East Bay Municipal Utilities District (EBMUD) representatives
- Reviewed reports, presentations, and documents provided by EBMUD and CCWD through requests for information
- Researched documents available on the EBMUD website (www.ebmud.com), CCWD website (www.ccwater.com), and other related websites listed in the reference section of this report
- Conducted an on-site review of sensitive documents and discussed the contents with district staff

BACKGROUND

Terrorism is the unlawful use of force and violence against a government or agency in furtherance of political or social objectives. The terrorist attacks on September 11, 2001, led to a heightened awareness of threats and the subsequent creation of the Department of Homeland Security (DHS). Its charter included identifying and preventing all forms of cyberattacks. The ransomware attacks on the Contra Costa Library system and the Pittsburg Unified School District are examples of recent cyberattacks in Contra Costa County. Cyberattacks compromise an organization's information technology (IT) or operational technology (OT) systems, preventing the organization from accomplishing its mission. WaterISAC is the information sharing and operational arm of the U.S. water and wastewater sector. It states these attacks can take any of the following forms:

- Successful ransomware attacks or close calls
- Successful installations of malware that had or may have had an impact on the utility's ability to conduct business and operations
- Phishing campaigns (sending fraudulent communications that appear to come from a reputable source), including successful or attempted spear-phishing of executives and key personnel
- Data thefts

- Social engineering (the use of deception to manipulate individuals into divulging confidential or personal information for fraudulent purposes) in an attempt to gather sensitive information (2019, pp. 3-4)

Federal Response to Cyberattacks

In 2003, Homeland Security Presidential Directive 7 required federal agencies to identify critical national infrastructures. The Directive established the U.S. Environmental Protection Agency (EPA) as the designated agency to protect water infrastructure. Over time, the EPA's role changed from physical protection of reservoirs, pipelines, and treatment plants to safeguarding against a multitude of malevolent attacks. These include cyberattacks on the computers of the industrial control systems (ICS) used in all modern water systems. The EPA issued the Water Security Research and Technical Support Action Plan in 2003, guiding the current state of research into water security.

In February 2013, President Obama issued Executive Order 13636: *Improving Critical Infrastructure Cybersecurity*, which recognized that cyberattacks “have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.” (p. 11741). The Cybersecurity Enhancement Act of 2014 formalized the National Institute of Standards and Technology's (NIST) role in developing a voluntary framework for all industries to identify, assess, and manage cyber risks. (2018, p. 1). Both the EPA and NIST continue to publish and encourage enterprises to follow cybersecurity guidelines voluntarily.

In 2018, the DHS, Cyber Security Division, issued an alert stating Russia was actively targeting American infrastructure to include “energy, nuclear, commercial facilities, water, aviation, and critical manufacturing sectors.” (2018, p.1). The alert notified thousands of network defenders around the United States to better defend against a Russian attack. It listed the tactics, techniques, and procedures employed by terrorists to circumvent IT firewalls and attack OT systems. Attacks on the OT systems disable the ICS used by all modern water treatment facilities that control the valves and chemicals to treat drinking water.

Federal Law Becomes Directive

In 2018, President Trump signed the American Water Infrastructure Act (AWIA) protecting community water systems from cyberattacks, among other things. All water systems serving over 3,300 customers must comply. Section 2013 of the AWIA provides for:

- **Risk and Resilience Assessments (RRA)** – The assessment must include:
 - The risk to the system from malevolent acts and natural hazards
 - The resilience of all physical infrastructure to source, transfer, and treat drinking water; and electronic, computer, or other automated systems (including the security of such systems)

- Monitoring practices of the system
- The financial infrastructure of the system
- Use, storage, or handling of various chemicals by the system
- Operation and maintenance of the system
- **Baseline Information** – The EPA provided this information in August 2019, and defined what constitutes malevolent acts on a community water system:
 - Substantially disrupt the ability of the system to provide a safe and reliable supply of drinking water
 - Otherwise, present significant public health or economic concerns to the community served by the system
- **Certification** – Using EPA’s Baseline Information, each community water system completes its RRA certifying that it complies. It then submits the RRA to the EPA by March 31, 2020, for systems serving a population of 100,000 or more. See Appendix for a copy of the RRA certification form.
- **Emergency Response Plan (ERP)** – The plan incorporates the findings of the RRA. The plan must be completed and certified to the EPA within six months after the RRA. See Appendix for a copy of the ERP certification form. The ERP must consist of:
 - Strategies and resources to improve the resilience of the system, including the physical security and cybersecurity of the system
 - The identification and implementation of plans and procedures used in the event of a malevolent act or natural disaster that threatens the community water system’s ability to deliver safe drinking water
 - Procedures to lessen the impact of a malevolent act or natural hazard on public drinking water
 - Strategies to aid in the detection of malevolent acts or natural hazards that threaten the security or resilience of the system
- **Technical Assistance and Grants** – This provision establishes the Drinking Water Infrastructure Risk and Resilience Program to award grants in 2020 and 2021. The community water system agrees to use the grant funds exclusively to assist in the planning, design, construction, or implementation of a program or project supporting its ERP (U.S. Congress, 2018). Otherwise, costs for these upgrades might be passed on to the water district’s customers.

The U.S. has over 151,000 water districts, making it difficult to prevent every cyber-attack. The Grand Jury reviewed the cyberattack preparedness of Contra Costa’s two largest water districts: Contra Costa Water District and East Bay Municipal Utilities District.

Contra Costa County's Water Districts

The Contra Costa Local Agency Formation Commission (LAFCO) authorized the organization of CCWD (2013, p. 99). CCWD has 500,000 customers (44% of the County's population) in its 220 square mile service area (Figure 1). It is the largest water district in the County and one of the largest urban water districts in the state. CCWD provides treated water to approximately 200,000 customers in Clayton, Clyde, Concord, Pacheco, Port Costa, and parts of Martinez, Pleasant Hill, and Walnut Creek. As a wholesaler, CCWD provides treated water to Antioch, Bay Point, and a portion of Brentwood. Additionally, it provides wholesale untreated water to the cities of Antioch, Martinez, and Pittsburg (CCWD, 2016, p. 1-1).

CCWD receives water from the Sacramento-San Joaquin Delta through four separate intakes. It then moves water through the 48-mile Contra Costa Canal, which starts at Rock Slough and ends at the Martinez Reservoir. Los Vaqueros Reservoir acts as the District's primary water storage. On July 24, 2018, CCWD announced that the California Water Commission gave \$459 million of Proposition 1 funding to expand Los Vaqueros Reservoir to 275,000 acre-feet, nearly doubling its capacity. A five-member elected Board of Directors (BOD) governs the district.

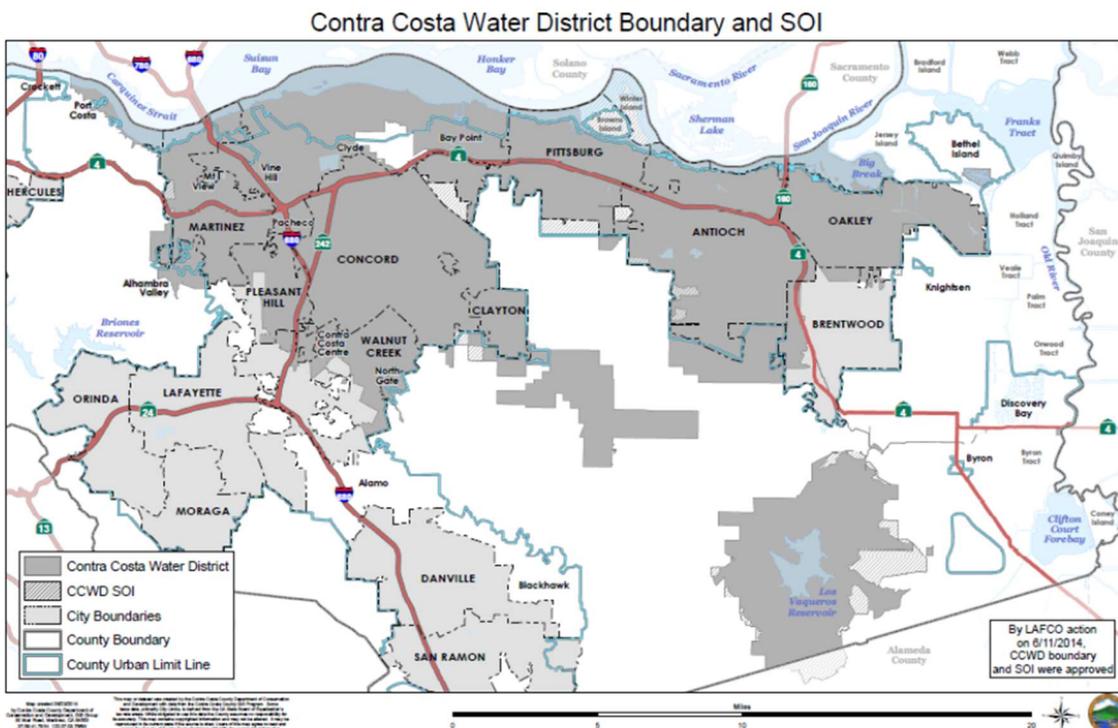


Figure 1. CCWD Service Area, 2014

The Alameda County LAFCO authorized the organization of EBMUD. It covers a 332-square-mile service area in Contra Costa and Alameda Counties (Figure 2). In Contra Costa County, EBMUD has a 146 square-mile service area with 470,000 customers, or 39% of the County's population. The district serves the following communities in Contra Costa County: Alamo, Danville, Crockett, El Cerrito, Kensington, Hercules, Lafayette, Moraga, Orinda, Pinole, Richmond, Rodeo, San Ramon, and Walnut Creek. EBMUD receives its water from the Mokelumne River watershed in the Sierra Nevada mountains. Two large reservoirs in the Sierra foothills store water until it moves to the East Bay for treatment and distribution. A seven-member elected BOD governs the district, with five members representing a portion of Contra Costa County.

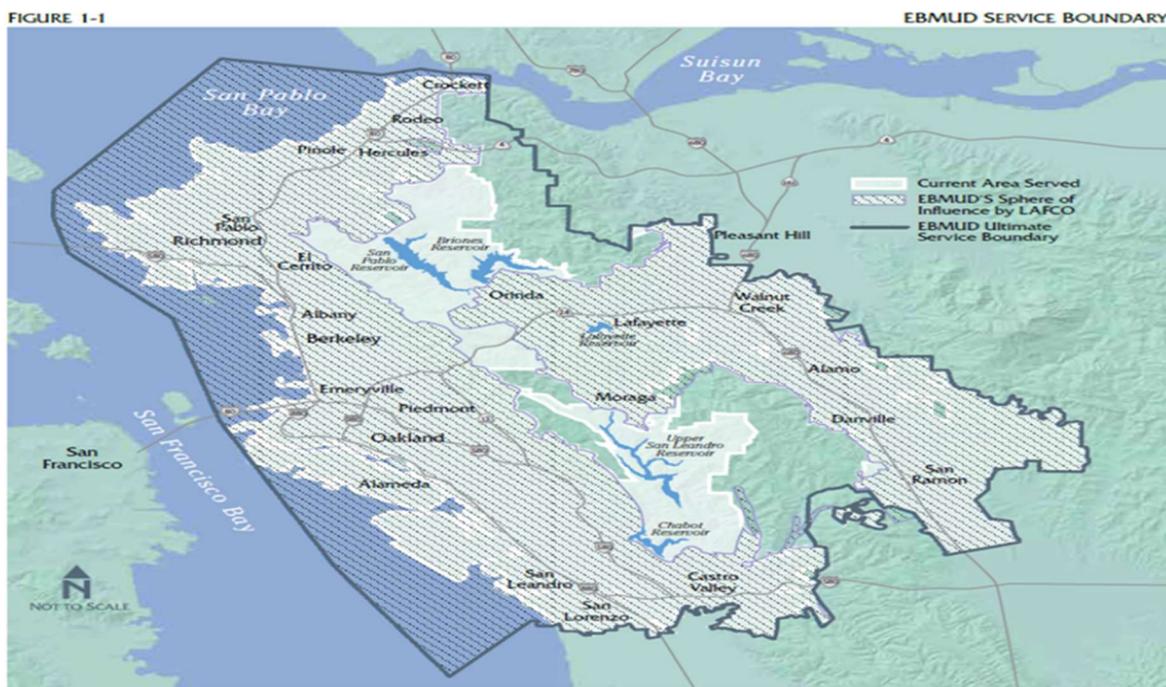


Figure 2 EBMUD Service Area Alameda and Contra Costa Counties

DISCUSSION

This investigation examined how Contra Costa's two largest water districts protect the public drinking water from cyberattacks. It focused on compliance with AWIA's requirement for the RRA and its certification by March 31, 2020, and preparation of the ERP by August 31, 2020. The AWIA does not require the public release of the actual RRA, but the certification requires the districts to meet EPA Baseline Standards, issued in August 2019. The Grand Jury asked the districts for information on their approach, plans to meet the law, and when they would complete the required work.

EPA Guidance

The EPA developed a guidance document to provide baseline information regarding malevolent acts of relevance to community water systems (EPA, 2019a). The AWIA does not specify standards, methods, or tools to complete the RRA. However, the EPA “recommends the use of standards, including the American Water Works Association’s J100-10 Risk and Resilience Management of Water and Wastewater Systems, along with tools from the U.S. EPA (e.g., VSAT) and other organizations, to facilitate sound risk and resilience assessments.” (EPA, 2019b).

The EPA created a series of documents, tutorials, web-based assessment tools, and websites all designed to meet AWIA, Section 2013 requirements:

- America’s Water Infrastructure Act of 2018 (AWIA): Overview
- America's Water Infrastructure Act: Risk Assessments and Emergency Response Plans
- Drinking Water or Wastewater Utility Risk Assessment: Vulnerability Self-Assessment Tool - Web-Enabled (VSAT Web) 2.0

EBMUD and CCWD must comply with the EPA Baseline Information guidance and complete the certification by March 31, 2020. Given the scope of the RRA outlined in the background of this report, the use of EPA’s VSAT Web will assist the water districts in completing their assessment. Although third party standards are not mandated, EPA’s recommendation to follow American Water Works Association’s (AWWA’s) J100-10 standard will help the water districts in completing their assessment and meeting the requirements of AWIA.

EBMUD

EBMUD maintains its IT and OT hardware, software, and protections using commercial off-the-shelf (COTS) components. The OT is separate from the IT, and EBMUD indicated that this element to the ICS exceeds current industry practices. As an example, EBMUD does not connect mobile devices used to maintain the system to the Internet. This physical separation of IT from the OT hinders inserting malware into the ICS.

EBMUD initiated an internal vulnerability assessment in 2014 and published its findings in 2015. The assessment remains the key to its cyberattack mitigation strategy. AWIA does not preclude the use of old assessments. EPA cautions: “If the water system has omitted, modified, or added components that must be addressed under AWIA, then the water system must assess the risk to and resilience of the omitted, modified, or added components before certifying the assessment.” (2019b, p. 2).

As a result of the 2015 vulnerability assessment, EBMUD conducts on-going audits and upgrades to mitigate the issues raised in the report. The district assesses itself to be at NIST Tier 3, Repeatable (subject to EPA audit). According to NIST (2018, p. 8): “Tiers

describe an increasing degree of rigor and sophistication in cybersecurity risk management practices. They help determine the extent to which cybersecurity risk management is informed by business needs and is integrated into an organization's overall risk management practices." Tier 3 is next to the highest rating established by NIST. The Grand Jury commends EBMUD for maintaining this standard.

EBMUD has organized a project team within its Regulatory Compliance Division. Members of that team completed certification in AWWA's Utility Risk and Resilience Program. EBMUD intends to map existing documents into the AWWA J100-10 framework to meet the RRA requirement. EPA recommends using the AWWA J100-10 standard in meeting the RRA requirement (2019b, p. 2). The Grand Jury commends EBMUD for following this guidance. EBMUD must determine if the 2015 vulnerability assessment comprehensively meets the requirements of AWIA.

EBMUD will use its existing Emergency Operations Plan and Business Continuity Plan to fulfill the ERP requirement. EBMUD may modify these plans as part of the RRA. EPA provides the Vulnerability Self-Assessment Tool - Web-Enabled (VSAT Web) 2.0 to assist in this work.

The Drinking Water Infrastructure Risk and Resilience Program provides grants in 2020 and 2021 to increase the resilience of water systems based on ERP requirements. These grants will help offset water rate increases that customers might otherwise pay. EBMUD should consider using this program to gain federal funding to improve the resilience of its water system.

EBMUD's public website has no information on its physical security or cybersecurity program, and a web search at the time of this report's publication revealed only one document published in 2012. However, the document does not reflect the vulnerability assessment reported in 2015, the current investment in cybersecurity, or the efforts to comply with AWIA. Information about cyber security informs the public of the ongoing cyber threat and what EBMUD is doing to counter that threat.

CCWD

CCWD maintains its IT and OT hardware, software, and protections using COTS components. The Grand Jury investigation did not indicate if CCWD's IT and OT systems were physically separate. One security feature CCWD did state was that its vehicle area network allowed crews to connect their computers to the OT network while at job sites.

CCWD has not officially adopted AWWA G430 Utility Management Standards, but its internal program to reduce cyberattack vulnerability conforms to this standard. CCWD also stated it generally adheres to the NIST Framework (2018), with the following elements applicable to cybersecurity:

- Key personnel receive regular training on current cybersecurity issues, vulnerabilities, and threats. There is a security check to comply with the federal

Bioterrorism Act of 2002. A third-party vendor completes an annual cybersecurity review and risk assessment.

- Critical systems are physically separated. Both physical and computer systems maintain access control. The staff receives regular cybersecurity awareness training.
- CCWD continuously monitors and audits access logs to all systems.
- Response plans exist, and the staff routinely conducts exercises. Emergency response capability is continuously maintained.
- There is a recovery plan for critical data, and there are redundant backups.

The Grand Jury commends CCWD for training its personnel on cybersecurity issues and exercise of its emergency response plans. CCWD's responses in other areas require further explanation.

- AWIA's RRA replaces the Bioterrorism Act's vulnerability assessment and certification (Federal Register, 2019, pp. 11536-11538). Therefore, any activity in support of the Bioterrorism Act will no longer be required. The CCWD list of contracts did not list the third-party annual cybersecurity review and risk assessment.
- CCWD did not define its critical systems. The separation of IT from the OT systems hinders the introduction of malware into its operations.
- The Grand Jury specifically asked CCWD to define and show the Tier level it has achieved as part of the NIST Framework. The tiers determine if the business needs to inform its cybersecurity risk management. CCWD did not identify what Tier it has reached. CCWD did not explain its rationale on the NIST Tier level.

CCWD's staff participated in the following training to support the RRA and ERP projects:

- EPA-led training in RRA and ERP requirements
- EPA-led training on earthquake threat mitigation
- Consultant-led training on the importance of AWIA

CCWD issued a memo on March 11, 2020, detailing its plan to conform to the requirements of AWIA. CCWD acknowledged AWIA supersedes the 2002 Bioterrorism Act, and its compliance activities focus on AWIA. CCWD intends to address all the risk categories of the RRA and limit natural hazards to those expected in Contra Costa County: earthquakes, wildfires, floods, power outages, and drought. CCWD will assess all asset categories (pipes, treatment centers, electronic, computer, and all automated systems, etc.). CCWD will aggregate its existing plans and publications into a Reference Document Table. It will then create a Compliance Report using two matrices – one for natural threats and one for malevolent threats. CCWD was expected to submit the Compliance Report to the EPA by March 31, 2020, to meet the RRA certification requirement. CCWD must comply with the Baseline Standards established by the EPA.

EPA's guidance and creation of the VSAT Web tool for self-assessment and recommendation to follow the AWWA J100-10 standard provide CCWD with the tools necessary to complete the RRA if the district decides to use them. The Grand Jury compared the information CCWD supplied with the required assessment under EPA's RRA certificate (see Appendix) - it met all the assessment criteria. CCWD has not published its RRA certificate on its public website.

The Drinking Water Infrastructure Risk and Resilience Program provides grants in 2020 and 2021 to increase the resilience of water systems based on ERP requirements. These grants will help offset water rate increases that otherwise customers would pay. CCWD should consider using this program to gain federal funding to improve the resilience of its water system.

CCWD published the memo described above detailing its compliance with AWIA. Other than this new memo, there is no mention on its website informing the public of the current cyber threat. Although the memo details CCWD's response to AWIA, it is an attachment to the minutes of a Board meeting. A prominent public statement would give residents an understanding of the commitment and effort CCWD makes to defend against cyberattacks.

FINDINGS

- F1. EBMUD's response to the American Water Infrastructure Act is timely and conforms to all requirements of this Act.
- F2. EBMUD's use of staff rather than an outside consultant for the Risk and Resilience Assessment complies with the American Water Infrastructure Act requirements.
- F3. EBMUD expects to reuse existing plans to comply with the American Water Infrastructure Act Emergency Response Plan. The Act does not discuss the reuse of existing plans, and the impact on EBMUD's certification cannot be determined.
- F4. EBMUD's public security notice on its website does not include a discussion about previous risk assessments.
- F5. EBMUD's public security notice on its website does not discuss the American Water Infrastructure Act requirements, or how EBMUD intends to comply with this Act.
- F6. Federal funding is available through the Drinking Water Infrastructure Risk and Resilience Program that could strengthen EBMUD's cybersecurity infrastructure. These grants help offset water rate increases that customers might otherwise pay.
- F7. CCWD's response to the American Water Infrastructure Act is timely and conforms to all requirements of this Act.
- F8. CCWD's use of staff and an outside consultant for the Risk and Resilience Assessment complies with the American Water Infrastructure Act requirements.
- F9. CCWD's designated Risk and Resilience Assessment & Emergency Response Plan team received specific, relevant training in the areas specified under Section 2013 of the American Water Infrastructure Act.
- F10. There is no CCWD public website statement on the issue of cybersecurity or its program to counter cyberattacks.
- F11. The Grand Jury found no evidence regarding CCWD's National Institute of Standards and Technology Tier level. The National Institute of Standards and Technology Tier level is releasable to the public and essential to inform CCWD of how safe its water supply is from cyberattacks.
- F12. Federal funding is available through the Drinking Water Infrastructure Risk and Resilience Program that could strengthen CCWD's cybersecurity infrastructure. These grants help offset water rate increases that customers might otherwise pay.

RECOMMENDATIONS

Note: The Grand Jury conducted the majority of its investigation before Contra Costa County and the State of California issued shelter-in-place orders. The Jury recognizes that County departments, agencies, and cities are currently addressing COVID-19 related matters and the Jury has adjusted implementation dates in the recommendations accordingly.

- R1. EBMUD Board of Directors should consider publishing a cyber policy acknowledging the cyberattack threat and informing the public of its programs to overcome and prevent attacks on the public water supply by December 31, 2020.
- R2. EBMUD Board of Directors should consider publishing its conformance with the American Water Infrastructure Act on its public webpage by December 31, 2020.
- R3. EBMUD Board of Directors should consider applying for a grant to offset new technology costs and strengthen its cybersecurity infrastructure under the Drinking Water Infrastructure Risk and Resilience Program by December 31, 2020.
- R4. CCWD Board of Directors should consider publishing a cyber policy acknowledging the cyberattack threat and informing the public of its programs to overcome and prevent attacks on the public water supply by December 31, 2020.
- R5. CCWD Board of Directors should consider applying for a grant to offset new technology costs and strengthen its cybersecurity infrastructure under the Drinking Water Infrastructure Risk and Resilience Program by December 31, 2020.

REQUIRED RESPONSES

	Findings	Recommendations
EBMUD Board of Directors	F1 - F6	R1 - R3
CCWD Board of Directors	F7 - F12	R4 - R5

These responses must be provided in the format and by the date set forth in the cover letter that accompanies this report. An electronic copy of these responses in the form of a Word document should be sent by e-mail to ctadmin@contracosta.courts.ca.gov, and a hard (paper) copy should be sent to:

Civil Grand Jury – Foreperson
725 Court Street
P.O. Box 431
Martinez, CA 94553-0091

Appendix

References

Clark, R. M., Panguluri, S., Nelson, T. D., & Wyman, R. P. (2016). *Protecting drinking water from cyber threats*. Washington, D.C. Idaho National Laboratory, INL/JOU-16-39302.

Contra Costa LAFCO. (2013). *Directory of local agencies: Water districts*. Retrieved from http://www.contracostalafco.org/documents/local_agency_directory_2013/Sect%2016%20-%20Water%20Districts%202013%20rev%207-14.pdf

CCWD. (2016). *2015 Urban water management plan for the Contra Costa Water District*. Retrieved from <https://www.ccwater.com/DocumentCenter/View/2216/2015-Urban-Water-Management-Plan-PDF>.

CCWD. (2020). *America's water infrastructure act of 2018 update*. Retrieved from <https://www.ccwater.com/DocumentCenter/View/8247/031120-1-Americas-Water-Infrastructure-Act-Update?bidId=>

EBMUD. (2012). *Measures that protect drinking water supplies*. Retrieved from https://www.ebmud.com/index.php/download_file/force/2273/1365/?security-fact-sheet-03-12.pdf.

EPA. (2019a). *Baseline information on malevolent acts for community water systems*. Washington, D.C. Retrieved from

<https://www.epa.gov/waterriskassessment/baseline-information-malevolent-acts-community-water-systems>

EPA. (2019b). *Vulnerability self assessment tool: New requirements for drinking water utilities tutorial*. Washington, D.C. Retrieved from <https://www.epa.gov/water-riskassessment/conduct-drinking-water-or-wastewater-utility-risk-assessment>

Federal Register. (2019). *New risk assessment and emergency response plan requirements for community water systems*. Washington, DC. 84(59), 11536-11538. Retrieved from <https://www.epa.gov/waterresilience/new-risk-assessment-and-emergency-response-plan-requirements-community-water-systems>

NIST. (2018). *Framework for improving critical infrastructure cybersecurity*. National Institute of Standards and Technology. Washington, D.C. Retrieved from <https://doi.org/10.6028/NIST.CSWP.04162018>.

Obama, B. (2013). *Executive Order 13636 of February 12, 2013: Improving critical infrastructure cybersecurity*. Federal Registry 78:33, pp 11739-11744. Retrieved from <https://www.govinfo.gov/content/pkg/FR-2013-02-19/pdf/2013-03915.pdf>

U.S. Congress. (2018). *America's Water Infrastructure Act of 2018, PL 115 – 270*. Retrieved from <https://www.congress.gov/bill/115th-congress/senate-bill/3021/text>

U.S. Department of Homeland Security, Cybersecurity, and Infrastructure Security Agency. (2018). *Russian government cyber activity targeting energy and other critical infrastructure sectors. Alert (TA18-074A)*. Washington, D.C. Retrieved from <https://www.us-cert.gov/ncas/alerts/TA18-074A>

WaterISAC. (2019). *15 Cybersecurity fundamentals for water and wastewater utilities*. Washington, D.C.: Water Information Sharing and Analysis Center (WaterISAC). Retrieved from <https://www.waterisac.org/system/files/articles/15%20Cyber-security%20Fundamentals%20%28WaterISAC%29.pdf>

Acronyms

AWIA: American Water Infrastructure Act of 2018

AWWA: American Water Works Association

BOD: Board of Directors

CCWD: Contra Costa Water District

COTS: Commercial off-the-shelf

DHS: U.S. Department of Homeland Security

EBMUD: East Bay Municipal Utilities District

EPA: U.S. Environmental Protection Agency

ERP: Emergency Response Plan

ICS: Industrial control systems

IT: Information technology

LAFCO: Local Agency Formation Commission

NIST: National Institute of Standards and Technology

OT: Operational technology

RRA: Risk and Resilience Assessment

SOI: Sphere of Influence

EPA Risk and Resilience Assessment Certification Form

Certification of Community Water System Risk and Resilience Assessment in Compliance with America's Water Infrastructure Act of 2018

Part (A): Community Water System Identification

Community Water System Name: _____

Community Water System Complete Mailing Address: _____

Public Water System Identification Number: _____

Population Served: _____

Part (B): Certification Date

Date of the certification: _____

Part (C): Certification Statement

I, _____

[Name of certifying official]

hereby certify that the community water system named under Part A, above, has *[select all that apply]*

conducted reviewed reviewed and revised

an assessment of the risks to, and resilience of, its system. This assessment included an assessment of:

1. The risk to the system from malevolent acts and natural hazards;
2. The resilience of the pipes and constructed conveyances, physical barriers, source water, water collection and intake, pretreatment, treatment, storage and distribution facilities, electronic, computer, or other automated systems (including the security of such systems) which are utilized by the system;
3. The monitoring practices of the system;
4. The financial infrastructure of the system;
5. The use, storage, or handling of various chemicals by the system; and
6. The operation and maintenance of the system; and
7. Optionally, may include an evaluation of capital and operational needs for risk and resilience management for the system.

[Signature of certifying official - click to add a digital signature, or print and sign]

EPA Emergency Response Plan Certification Form

Certification of Community Water System Emergency Response Plan in Compliance with America's Water Infrastructure Act of 2018

Part (A): Community Water System Identification

Community Water System Name: _____

Community Water System Complete Mailing Address: _____

Public Water System Identification Number: _____

Population Served: _____

Part (B): Certification Date

Date of the certification: _____

Part (C): Certification Statement

I, _____

[Name of certifying official]

hereby certify that the community water system named under Part A has completed an emergency response plan that incorporates findings of the risk and resilience assessment conducted under Section 2013(a) of America's Water Infrastructure Act of 2018 for such system (and any revisions thereto). This emergency response plan includes:

1. Strategies and resources to improve the resilience of the system, including the physical security and cybersecurity of the system;
2. 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 community water system to deliver safe drinking water;
3. Actions, procedures, and equipment which can obviate or significantly lessen the impact of a malevolent act or natural hazard on the public health and the safety and supply of drinking water provided to communities and individuals, including the development of alternative source water options, relocation of water intakes, and construction of flood protection barriers; and
4. Strategies that can be used to aid in the detection of malevolent acts or natural hazards that threaten the security or resilience of the system.

[Signature of certifying official - click to add a digital signature, or print and sign]