OFFICE OF THE STATE AUDITOR

DIANA DIZOGLIO

Official Audit Report – Issued August 25, 2023

Massachusetts Water Resources Authority

For the period July 1, 2019 through June 30, 2021

OFFICE OF THE STATE AUDITOR

DIANA DIZOGLIO

August 25, 2023

Frederick A. Laskey, Executive Director
Massachusetts Water Resources Authority
100 First Avenue, Building 39
Boston, MA 02129

Dear Mr. Laskey:

I am pleased to provide to you the results of the enclosed performance audit of the Massachusetts Water Resources Authority. As is typically the case, this report details the audit objectives, scope, methodology, findings, and recommendations for the audit period, July 1, 2019 through June 30, 2021. As you know, my audit team discussed the contents of this report with agency managers. This report reflects those comments.

I appreciate you and all your efforts at the Massachusetts Water Resources Authority. The cooperation and assistance provided to my staff during the audit went a long way toward a smooth process. Thank you for encouraging and making available your team. I am available to discuss this audit if you or your team have any questions.

Best regards,

Diana DiZoglio
Auditor of the Commonwealth

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

AWIA	America's Water Infrastructure Act
ERP	emergency response plan
ISP	information security program
MIS	Management Information System
MWRA	Massachusetts Water Resources Authority
RRA	risk and resilience assessment
SCADA	supervisory control and data acquisition
SPOC	single point of contact

EXECUTIVE SUMMARY

In accordance with Section 12 of Chapter 11 of the Massachusetts General Laws, the Office of the State Auditor has conducted a performance audit of the Massachusetts Water Resources Authority (MWRA) for the period July 1, 2019 through June 30, 2021.

The purpose of this audit was to determine whether MWRA implemented specific areas of its risk and resilience assessment[1] and emergency response plan[2]—certified on March 30, 2020 and September 29, 2020, respectively—in areas of information technology security, chemical delivery, and physical security in accordance with Section 2013 of the America's Water Infrastructure Act.

Below is a summary of our findings and recommendations, with links to each page listed.

Finding 1 **Page 13**	MWRA did not review and update its information security program (ISP) annually.
Recommendations **Page 13**	1. MWRA should review its ISP annually. 2. MWRA should develop and implement internal controls to ensure that it reviews its ISP annually.
Finding 2 **Page 14**	MWRA's single point of contact (SPOC) did not inform the Management Information System (MIS) Department of contractors' changes for user access and/or multifactor authentication statuses for its administrative computer network.
Recommendation **Page 15**	MWRA should develop a formal, written policy that includes monitoring controls and requires MWRA's SPOC to notify the MIS Department of contractors' user access and/or multifactor authentication statuses, including the authority to work remotely. MWRA should also train its employees on how to implement and follow this policy.
Finding 3 **Page 15**	MWRA did not ensure that all employees and contractors completed required cybersecurity awareness training for its administrative computer network.
Recommendation **Page 16**	MWRA should ensure that all its employees and contractors with access to its administrative computer network complete cybersecurity awareness training annually. MWRA should also implement internal controls to ensure that the employees and contractors complete the training.

1. According to the America's Water Infrastructure Act, a risk and resilience assessment evaluates the system's vulnerabilities, threats to the system, and consequences from potential hazards—for example, mold, pipe corrosion, or flooding.
2. According to the America's Water Infrastructure Act, an emergency response plan describes strategies, resources, plans, and procedures that MWRA can use to prepare for and respond to natural or man-made incidents that threaten life, property, or the environment—for example, a small main break or a hurricane.

Finding 4 **Page 17**	MWRA did not revoke employees' and contractors' access to its administrative computer network after their employment or contracted work ended.
Recommendation **Page 18**	MWRA should develop a written policy that includes monitoring controls and a 24–business hour timeframe to ensure that the SPOC informs the MIS Department about MWRA employees whose employment has ended and contractors whose contracts have ended. MWRA should also train its employees on how to implement and follow this policy.

OVERVIEW OF AUDITED ENTITY

The Massachusetts Legislature created the Massachusetts Water Resources Authority (MWRA) in 1985, in accordance with Chapter 372 of the Acts of 1984.

According to page 3 of MWRA's Comprehensive Annual Financial Report, dated October 19, 2021,

> *MWRA assumed control of the water and sewer systems, including facilities, properties, and the right to utilize water withdrawn from system reservoirs that had formerly been the Sewerage and Waterworks Divisions of the Commonwealth of Massachusetts ("the Commonwealth") Metropolitan District Commission (MDC). The Commonwealth, under the management of the MDC Watershed Management Division (now the Department of Conservation and Recreation – Division of Watershed Management), retained ownership of all real property comprising the water and sewer systems, including the reservoirs and watersheds, the maintenance of which are included in MWRA's operating budget. . . .*
>
> *MWRA's facilities span from the Quabbin Reservoir in western Massachusetts to the Deer Island Treatment Plant in Boston Harbor. In Fiscal Year 2021, the systems served approximately 3.1 million people and more than 5,500 businesses. . . .*
>
> *[Chapter 372 of the Acts of 1984] also established the MWRA Advisory Board to represent the cities and towns in the service area. The Advisory Board appoints three members to the MWRA Board of Directors, approves the extension of water and sewer services to additional communities, and reviews and makes recommendations on MWRA's annual Current Expense Budget and Capital Improvement Program.*

MWRA is governed by an 11-member board of directors (three members appointed by the Governor, three members appointed by MWRA's advisory board, three members appointed by the mayor of Boston, one member appointed by the mayor of Quincy, and one member appointed by the town council president of Winthrop). According to its website,

> *MWRA's mission is to provide reliable, cost-effective, high-quality water and sewer services that protect public health, promote environmental stewardship, maintain customer confidence, and support a prosperous economy. . . . MWRA . . . provides wholesale water and sewer services to its customer communities, and funds its operations primarily through user assessments and charges.*

Total operating revenue for fiscal years 2019 and 2020 was approximately $755.3 and $778.3 million, respectively. Of these amounts, rate revenue[3] was $739 and $760.9 million, respectively.

3. Rate revenue includes charges for water and sewer services. Water rates are set through the cost to run the water system, and sewer rates are computed on a proportional allocation basis using total flow.

Oversight and Monitoring of Water Systems

The United States Environmental Protection Agency, the Massachusetts Department of Environmental Protection, and other enforcement agencies work together to implement environmental standards set by the United States Clean Water Act (for wastewater) and the Safe Drinking Water Act (for drinking water). These agencies also perform various monitoring processes with MWRA to keep the water, the process of treating the water, and the disposal processes of wastewater safe for communities in the Commonwealth. Constant monitoring of systems is essential to keep the Commonwealth's water clean and safe.

America's Water Infrastructure Act

MWRA undergoes a certification process in accordance with the America's Water Infrastructure Act (AWIA), which has a five-year cycle for recertification. According to the AWIA, "Each community water system serving a population of greater than 3,300 persons shall conduct an assessment of the risks to, and resilience of, its system . . . to provide a safe and reliable supply of drinking water."

According to the United States Environmental Protection Agency's webpage on the AWIA, "No later than six months after certifying completion of its risk and resilience assessment, each system must prepare or revise, where necessary, an emergency response plan."

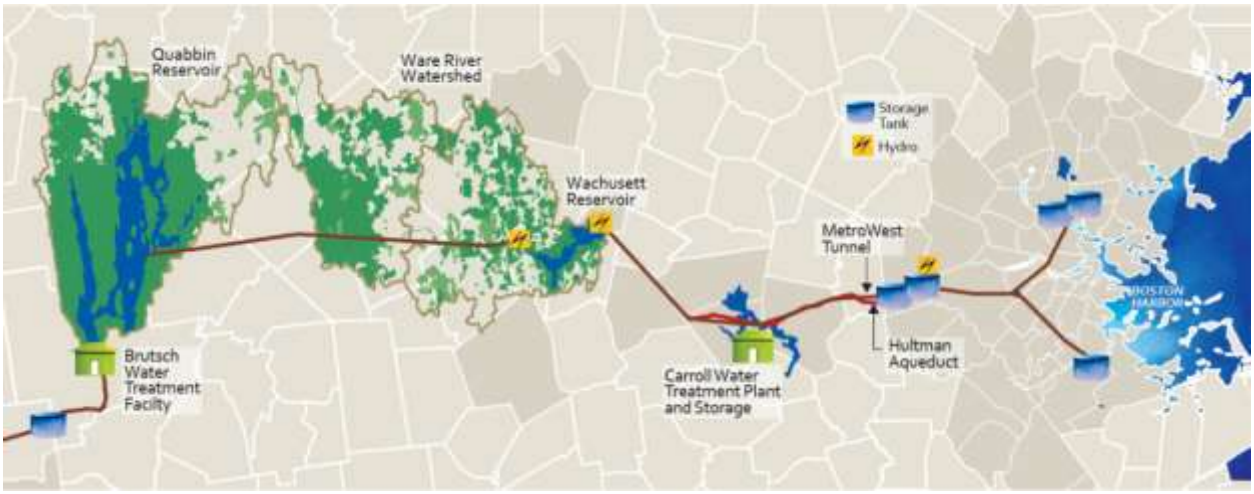
Water Treatment Plants

The John J. Carroll Water Treatment Plant in Marlborough treats water for most MWRA communities with ozone and ultraviolet light[4] as well as other chemicals. The treated water leaves the plant through the MetroWest Water Supply Tunnel and the Hultman Aqueduct. Along the way, it is stored in covered storage tanks. Three MWRA communities—Chicopee, an area in South Hadley, and Wilbraham—have their water treated at the William A. Brutsch Water Treatment Facility in Ware, and the water leaves the plant through the Chicopee Valley Aqueduct.

MWRA's website states, "MWRA's water comes from the Quabbin Reservoir, about 65 miles west of Boston, and the Wachusett Reservoir, about 35 miles west of Boston. . . . The Quabbin alone can hold a . . . five-year supply of water."

4. According to MWRA, "Ozone disinfects the water, killing pathogens and oxidizing some other contaminants. Ultraviolet light disinfects water by inactivating chemical- resistant pathogens."

MWRA's Water System



Source: MWRA (https://www.mwra.com/04water/html/watsys.htm)

Water Treatment

MWRA's website states, "MWRA tests over 1,600 water samples per month, from the reservoirs all the way to household taps." MWRA uses process and laboratory testing to ensure that water is safely treated with chemicals and has protocols to ensure the safety of its staff members.

According to MWRA's website, "MWRA's licensed treatment operators treat drinking water according to strict state and federal regulations." The following table provides details on some of the treatments/chemicals that MWRA uses on its drinking water.

Treatment	Purpose
Ozone	Primary disinfectant (to achieve 99.9% *Giardia* inactivation)
Sodium Bisulfite	To remove ozone
Ultraviolet Light	Second primary disinfectant, to inactivate chemically resistant parasites, such as *Cryptosporidium*
Sodium Hypochlorite (Chlorine)	For residual disinfection, to protect water as it travels through the pipe network
Hydrofluorosilicic Acid (Fluoride)	For dental health
Aqueous Ammonia	To combine with chlorine to form monochloramine for residual disinfection
Sodium Carbonate	To raise the alkalinity of the water for pH buffering; to minimize lead and copper leaching
Carbon Dioxide	To adjust pH to final level

Source: MWRA (https://www.mwra.com/04water/html/watsys.htm)

Drinking water is dispersed through 13 covered storage facilities, which are listed from largest to smallest size, in the following table.

Covered Storage Facility	Location	Gallons Held (millions)
Norumbega	Weston	115
Carroll	Marlborough	45
Nash Hill	Ludlow	25
Blue Hills	Milton	20
Fells	Stoneham	20
Spot Pond	Stoneham	20
Loring Road	Weston	20
Arlington	Arlington	2
Bear Hill	Stoneham	6
Bellevue	West Roxbury (Boston)	3.7
Deer Island	Deer Island (Boston)	2
Turkey Hill	Arlington	2
Walnut Hill	Lexington	2
Total		**282.7**

Physical Security of Water Treatment Facilities

According to MWRA officials, all MWRA employees are issued employee access identification cards. Their identification cards are badges that provide access to any building or facility and must be worn while they are on duty. Access points requiring badges are monitored.

A contractor programs the electronic access control system to provide door alarm monitoring for entrances to sensitive areas in MWRA facilities. MWRA security personnel stated that MWRA uses cameras, fences, locked gates, and deterrence signage for its physical security and that contractors are told to respond to any alarms.

MWRA contracts with third-party vendors to maintain the security of its facilities. Each vendor provides a specific component of security, including staffing, badge tracking, and camera/video monitoring.

Information Systems and Cybersecurity

MWRA has technical infrastructure systems—including MWRA's administrative computer network and a separate process control system, a supervisory control and data acquisition (SCADA) system[5]—for operating the water treatment plants and pipelines. MWRA stated in a letter in response to our draft audit report, dated June 16, 2023, "Access to the SCADA system is only available within MWRA facilities and only by a small group of trained operational staff."

According to MWRA officials, the Human Resources and Management Information System (MIS) Departments provide access to its systems using multifactor authentication for MWRA employees and contractors, conduct trainings on using the systems, and revoke access to the systems when appropriate. MWRA has established an information security program to outline requirements for system users. Contractors receive access through an MWRA employee, called the single point of contact (SPOC). The SPOC initiates remote access requests for contractors as needed (for example, when a contractor performs security system maintenance and equipment installation). The SPOC submits a request for authorization of remote access for the identified contractor. The director of the MIS Department approves all requests for authorization of remote access.

Upon the director's approval of the request for authorization of remote access, the MIS Department creates an account for the contractor. Access is limited to the system(s) they are contracted to use. When the contractor no longer needs access to a system, the SPOC notifies the MIS Department that the access is no longer needed and the MIS Department deletes the account.

5. A SCADA system gathers data from computers, transmitters, and other instruments.

AUDIT OBJECTIVES, SCOPE, AND METHODOLOGY

In accordance with Section 12 of Chapter 11 of the Massachusetts General Laws, the Office of the State Auditor has conducted a performance audit of certain activities of the Massachusetts Water Resources Authority (MWRA) for the period July 1, 2019 through June 30, 2021.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Below is a list of our audit objectives, indicating each question we intended our audit to answer; the conclusion we reached regarding each objective; and, if applicable, where each objective is discussed in the audit findings.

Objective	Conclusion
1. Did MWRA implement a risk and resilience assessment (RRA) for its administrative computer network and supervisory control and data acquisition (SCADA) system in the areas of authorized employee access that support the monitoring of drinking water and wastewater, as required by Section 2013 of the America's Water Infrastructure Act (AWIA)?	No, see Findings 1, 2, 3, and 4
2. Did MWRA implement an RRA as it pertains to the use, storage, delivery, or handling of the six chemicals used to treat water at the John J. Carroll Water Treatment Plant and William A. Brutsch Water Treatment Facility, as required by Section 2013 of the AWIA?	**Yes**
3. Did MWRA implement an emergency response plan (ERP) as it pertains to the resilience of physical security at the John J. Carroll Water Treatment Plant, Deer Island Treatment Plant, and Wachusett Reservoir, as required by Section 2013 of the AWIA?	**Yes**
4. Did MWRA have physical security measures in place to prevent unauthorized access to its water supply facilities and the Deer Island Treatment Plant?	**Yes**

To achieve our objectives, we gained an understanding of MWRA's internal control environment related to the objectives by reviewing applicable policies and procedures, as well as by interviewing MWRA's management and staff members. We evaluated the design and tested the effectiveness of MWRA's process of annually updating standard operating procedure(s) for the use, storage, delivery, or handling of the six chemicals to treat the water.

RRA—Network Access

To verify that MWRA implemented an RRA for its administrative computer network and its SCADA system, as required by Section 2013 of the AWIA, we performed the following procedures.

We obtained a Microsoft Excel list of the names of all 1,364 active and terminated users provided by MWRA's Human Resources Department. We stratified the list of active and terminated users into 1,342 administrative computer network users and 22 SCADA system users. We selected all 22 SCADA system users and selected a random, nonstatistical sample of 80 out of the 1,342 administrative computer network users.

- To determine whether users received authorization for access, we reviewed the Network Shared Permission Requests to verify each user's name and supervisor permission.
- To determine whether the Management Information System Department granted multifactor authentication to users, we compared the access permission granted for multifactor authentication to actual remote access usage.
- To confirm that employees and contractors completed cybersecurity awareness trainings, we reviewed each user's training completion dates in their account for two years of cybersecurity awareness training.
- In addition, we selected all nine terminated contractors and selected a random, nonstatistical sample of 35 out of 143 MWRA terminated employees with user access for a sample of 44 users. We compared the date of the end of their employment to the date of revoked access for each user and looked for timely deactivation of user access.

See Finding 1 for an issue we identified related to MWRA's information security program. See Findings 2, 3, and 4 for issues we identified related to MWRA's administrative computer network.

RRA—Chemical Use, Storage, Delivery, or Handling

We determined whether MWRA implemented an RRA as it pertains to the use, storage, delivery, or handling of the six identified chemicals used at the John J. Carroll Water Treatment Plant and William A. Brutsch Water Treatment Facility, as required by Section 2013 of the AWIA. To do this, we selected a random, nonstatistical sample of 95 out of 1,580 chemical deliveries from MWRA's Microsoft Excel list of all chemical deliveries.

For our testing, we compared the information for each chemical delivery in our sample to the corresponding vendor invoice. Information included the delivery date, the quantity of the chemical, the

amount paid, and a signature by an MWRA employee with signatory authority, which were on a bill of lading,[6] a certificate of analysis, an MWRA form (specific to the chemical), and the scale weight ticket included with each delivery. We also compared the volume calculation on the electronic scale ticket to the invoice volume and confirmed that the delivery documentation was accurate. We also reviewed the MWRA form and verified that it had the required MWRA receiver's signature at the line titled "Documentation Review and Delivery Hook-up."

We also selected a random, nonstatistical sample of 8 out of 24 months of the audit period and reviewed each month's Chemical Addition Report for each of the six chemicals, verified that each chemical was used daily, and verified that the report had the appropriate MWRA employees' signatures.

We noted no exceptions in our testing; therefore, we conclude that MWRA implemented an RRA as it pertains to the use, storage, delivery, or handling of the six chemicals used to treat water at the John J. Carroll Water Treatment Plant and William A. Brutsch Water Treatment Facility, as required by Section 2013 of the AWIA.

Emergency Response Plan

To determine whether MWRA implemented an ERP as it pertains to the resilience of physical security at the John J. Carroll Water Treatment Plant, Deer Island Treatment Plant, and Wachusett Reservoir, as required by Section 2013 of the AWIA, we selected a judgmental, nonstatistical sample of 20 physical security incidents[7] out of the 72 incidents that occurred during the audit period at any one of these three locations. We gathered information from cameras as well as badge and motion detector activity at various locations for each incident by date. We confirmed that MWRA had the physical security equipment (camera, badge, and motion detector) data related to the incidents.

We analyzed the total number of transactions (e.g., badge scans or activity captured by motion detectors) for each of the 20 incidents in the physical security equipment data by location and calculated the average number of transactions. We reviewed the description of the incidents for initiation of the ERP steps and for any unauthorized access to MWRA property.

6. A bill of lading is a list of the items (in this case, chemicals) in a shipment.
7. MWRA told us that a physical security incident is an event that violates MWRA policy or a law and/or compromises the safety of an MWRA employee, contractor, visitor, or MWRA property—for example, vandalism, theft, or accidental damage to MWRA property.

We performed site visits and observed physical security equipment at the John J. Carroll Water Treatment Plant and Deer Island Treatment Plant. We also reviewed evidence to support whether 24-hour security and deterrence signage methods were in place at multiple locations through interviews and direct observation.

We noted no exceptions in our testing; therefore, we conclude that MWRA implemented an ERP as it pertains to the resilience of physical security at the John J. Carroll Water Treatment Plant, Deer Island Treatment Plant, and Wachusett Reservoir, as required by Section 2013 of the AWIA.

Physical Security Measures

To determine whether MWRA had physical security measures in place to prevent unauthorized access to its water and wastewater facilities, we selected a random, nonstatistical sample of 35 incidents from a population of 203 incidents (from all of MWRA's facilities) during our audit period. We reviewed the details of the 35 incidents to determine whether the security of the water quality was directly affected or whether outside agencies, such as the state and local police, were called for assistance. We divided the 35 incident reports into three categories: significant, borderline, and insignificant, based on the type of incident. For the sample of 35 incidents, we determined whether MWRA's Security Department's responses to the incidents were in agreement with the defined protocols established in MWRA's "Security Guard After Hours Alarm and Event Handling." Based on MWRA's descriptions, we believed that six incidents appeared to be of a more significant nature than the other incidents. We assessed whether the contractor and/or MWRA employee took actions in accordance with MWRA's standard operating procedures. We inquired with MWRA, discussed its responses to these six incidents, and verified that the contractor and/or MWRA staff member followed the steps outlined within its ERP, if necessary.

We noted no exceptions in our testing; therefore, we conclude that MWRA had physical security measures in place to prevent unauthorized access to its water supply facilities and the Deer Island Treatment Plant.

When nonstatistical sampling methods were used, we could not project the results of our testing to the population.

Data Reliability Assessment

To determine the reliability of the Microsoft Excel list of names of active and terminated employees from MWRA's Human Resources Department, we reconciled the list to MWRA's payroll report list. We checked

the Microsoft Excel list of names for hidden rows and columns and/or formulas. We performed electronic tests for duplicate identification numbers and names within our audit period.

To determine the reliability of the Microsoft Excel list of all chemical deliveries that was exported from MWRA's procurement database, we filtered the deliveries for the six chemicals. We selected a random, nonstatistical sample of 20 out of 1,580 deliveries from the Microsoft Excel list of all chemical deliveries and traced each delivery to a bill of lading, certificate of analysis, and scale weight ticket. We also randomly selected source documents (bills of lading, certificates of analysis, and scale weight tickets) for 20 deliveries from MWRA files and traced the delivery information from those files to the Microsoft Excel list of all chemical deliveries. We also analyzed the chemical delivery list for hidden rows, columns, or formulas. We used Audit Command Language to check for duplicate data in our audit period and check that there were no large gaps in data files.

To determine the reliability of the badge, camera, and motion detector data obtained from the contractor who provided the security data system / database, we reconciled the data pulled on a specific date to the total of all transactions that we received. We also inspected the data (representing badges, cameras, and motion detectors) for hidden rows, columns, or formulas and imported the data into the Audit Command Language data analytics system. We tested for duplicates and dates outside the audit period.

To determine the reliability of the list of incidents tracked by MWRA's director of security during the audit period, we selected a random, nonstatistical sample of 10 out of 203 incidents from the list and traced them to Security Incident Reports. We randomly selected a nonstatistical sample of 10 Security Incident Reports and traced the incident identification number and description of the incident from the reports to the list of incidents. We performed other electronic tests, including checking for hidden rows, columns, or formulas; checking that data was in our audit period; testing for duplicates; and testing for large gaps.

Based on the results of our data reliability assessment, we determined that the information obtained for our audit period was sufficiently reliable for the purposes of the audit.

DETAILED AUDIT FINDINGS WITH AUDITEE'S RESPONSE

1. The Massachusetts Water Resources Authority did not review and update its information security program annually.

During our audit, we reviewed the Massachusetts Water Resources Authority's (MWRA's) information security program (ISP) and determined that it had not been reviewed annually. Specifically, Policy ADM.30 (MWRA Information Technology User Responsibilities) and Policy ADM.31 (MWRA Information Security Policy) of MWRA's ISP were last reviewed in 2017.

As a result, there is a higher-than-acceptable risk that MWRA's information systems may not be adequately protected from vulnerabilities, which could result in the loss of protected information.

Authoritative Guidance

According to Policy ADM.31, "The ISP will be reviewed annually."

Reasons for Issue

MWRA officials told us they were not aware of the requirement to do an annual review of the ISP. Additionally, MWRA did not have internal controls in place to ensure that it reviewed the ISP.

Recommendations

1. MWRA should review its ISP annually.
2. MWRA should develop and implement internal controls to ensure that it reviews its ISP annually.

Auditee's Response

MWRA has comprehensively revised its Information Security Policy ADM.31*, including additional requirements on annual updating processes, required staff training, roles and responsibilities, and enforcement mechanisms. That policy review was already underway while the audit was being conducted. The revised policy is undergoing final senior management review and is anticipated to be approved before the end of June. While the policy itself had not been formally reviewed annually, MWRA's Information Security Council, made up of senior staff from process controls, administrative and physical security, meets monthly to discuss events in cyber and physical security and their impact on MWRA policies and procedures. Following the Department of Homeland Security's recommended best practices, MWRA has a process for distributing and installing security upgrades and patches to all systems.*

MWRA internal audit staff will develop and implement the necessary internal controls to ensure that annual reviews of the policy are conducted.

Auditor's Reply

Based on its response, MWRA is taking measures to address our concerns on this matter.

2. The Massachusetts Water Resources Authority's single point of contact did not inform the Management Information System Department of contractors' changes for user access and/or multifactor authentication statuses for its administrative computer network.

MWRA's single point of contact (SPOC) did not inform MWRA's Management Information System (MIS) Department of six out of six contractors' user access and/or multifactor authentication statuses for its administrative computer network during contract work. The same six contractors, with approval from MWRA's SPOC for user access and/or remote work, were not approved to have remote access through the MIS Department.

As a result, there is a higher-than-acceptable risk that MWRA's administrative computer network may not be adequately protected from vulnerabilities, which could result in the loss of protected information.

Authoritative Guidance

Policy ADM.31 requires the following human resources security and access control:

> *This policy applies to all MWRA employees, business partners, and third party users that provide goods and services for MWRA [information technology (IT)] resources or shared environments, including the Supervisory Control and Data Acquisition (SCADA) System, Process Information Control System (PICS), Management Information System (MIS) and associated infrastructure components. . . .*
>
> *MWRA shall ensure that all of its employees, contractors, and third party users understand their security responsibilities and have the requisite skills and knowledge to perform effectively in the roles they are assigned, and to reduce the risk of unauthorized access, use, or modification of IT resources (theft, fraud or misuse of facilities). . . .*
>
> ***Access Control***
>
> *MWRA shall use controls for authorized access to information, IT resources, information processing facilities, and business processes on the basis of business and security requirements. Access control rules must take into account existing policies for information dissemination and authorization with consideration for the application of: . . .*
>
> - *Wireless and remote access controls*
> - *Controlled access and authentication to applications, systems, and networks*

MWRA officials told us in an email, dated September 19, 2022, that all SPOCs update the MIS Department on contractors' user access statuses.

Reasons for Issue

MWRA did not have a formal, written policy that includes monitoring controls and requires SPOCs to notify the MIS Department of contractors' user access and/or multifactor authentication statuses, including the authority to work remotely.

Recommendation

MWRA should develop a formal, written policy that includes monitoring controls and requires MWRA's SPOC to notify the MIS Department of contractors' user access and/or multifactor authentication statuses, including the authority to work remotely. MWRA should also train its employees on how to implement and follow this policy.

Auditee's Response

Contractors are only given access to the MWRA network if absolutely necessary for the conduct of their contracted scope of work. A new policy specifically addressing Contractors is in draft form, creating more formal processes for initially granting limited access, and terminating that access when it is no longer necessary for the completion of work. When the new policy is approved, all appropriate procurement, engineering and operational staff who oversee contractors will be trained on it to ensure that the appropriate controls are properly implemented for all contracts allowing access to MWRA networks.

It is important to note that no remote access to [MWRA's supervisory control and data acquisition system] or other water and wastewater control systems is ever permitted. The six contractor staff with access which was not terminated appropriately had been working on heating, ventilation and cooling (HVAC) systems and their access was terminated immediately after it was discovered.

Auditor's Reply

Based on its response, MWRA is taking measures to address our concerns on this matter.

3. The Massachusetts Water Resources Authority did not ensure that all employees and contractors completed required cybersecurity awareness training for its administrative computer network.

For fiscal year 2020, we identified 4 MWRA employees (out of a population of 102) and six contractors (out of a population of six) who had access to MWRA's administrative computer network but had not completed required annual cybersecurity awareness training. For fiscal year 2021, 2 MWRA employees

(out of a population of 102) and six contractors (out of a population of six) had access to MWRA's administrative computer network but had not completed the necessary annual cybersecurity awareness training.

A lack of such training may lead to user error and may compromise the integrity and security of protected information in MWRA's administrative computer network.

Authoritative Guidance

According to Policy ADM.31,

> *MWRA shall ensure that all of its employees, contractors, and third party users understand their security responsibilities and have the requisite skills and knowledge to perform effectively in the roles they are assigned, and to reduce the risk of unauthorized access, use, or modifications of [information technology] resources . . . including . . . Security awareness and training during employment.*

Section 6.2.4 of the Executive Office of Technology Services and Security's Information Security Risk Management Standard IS.010, which went into effect October 15, 2018, states,

> *All personnel will be required to complete Annual Security Awareness Training. Once implemented, automatic email reminders will be sent to* ***personnel*** *12 months after course completion, alerting* ***personnel*** *to annual refresher training completion deadlines.*

Although MWRA is not required to follow this standard, we consider it a best practice.

Reasons for Issue

MWRA officials told us that they overlooked the requirement in MWRA's ISP for contractors with access to its administrative computer network to complete cybersecurity awareness training. MWRA officials did not provide a reason why all employees did not complete required annual cybersecurity awareness training.

Recommendation

MWRA should ensure that all its employees and contractors with access to its administrative computer network complete cybersecurity awareness training annually. MWRA should also implement internal controls to ensure that the employees and contractors complete the training.

Auditee's Response

Supervisors and managers now receive a monthly report of staff that have not completed the required training. In [fiscal year 2022], 100% of MWRA staff successfully completed cybersecurity awareness training and MWRA is on track to achieve 100% completion for [fiscal year 2023]. Considerations are under review to modify the current cadence for the release and delivery of training modules to improve responsiveness without impacting operational schedules.

MWRA's existing training platform does not support students without MWRA domain email addresses, which currently limits our ability to have contractors directly use MWRA's cyber training materials. A review of the training system configuration will be conducted to accommodate Contractors, or an alternative approach developed.

Auditor's Reply

Based on its response, MWRA is taking measures to address our concerns on this matter.

4. The Massachusetts Water Resources Authority did not revoke employees' and contractors' access to its administrative computer network after their employment or contracted work ended.

During the audit period, MWRA did not revoke access to its administrative computer network within 24 business hours for 11 out of 35 employees upon the end of their employment. Additionally, the SPOC did not inform the MIS Department about eight out of eight contractors whose contracts had ended (and that, therefore, their access should be revoked).

As a result, MWRA's administrative computer network is potentially vulnerable to inappropriate use or misuse by employees whose employment has ended and contractors whose contracts have ended.

Authoritative Guidance

According to MWRA's Policy ADM.31,

MWRA shall ensure that all of its employees, contractors, and third party users understand their security responsibilities and have the requisite skills and knowledge to perform effectively in the roles they are assigned, and to reduce the risk of unauthorized access, use, or modification of [information technology] resources (theft, fraud or misuse of facilities).

According to Executive Office of Technology Services and Security's Access Management Standard IS.003,

6.1.8.3 If the termination date of personnel is known in advance, the respective access privileges — specifically those with access to confidential information — shall be configured to terminate automatically.

6.1.8.3.1 If not, access must be manually removed within 24 business hours.

Although MWRA is not required to follow this standard, we consider it a best practice.

MWRA officials told us in an email, dated September 19, 2022, that a SPOC requests the type of user access needed and updates the MIS Department on contractors' user access statuses.

Reasons for Issue

MWRA did not have a written policy that includes monitoring controls and a specific timeframe to ensure that the SPOC informed the MIS Department about MWRA employees whose employment had ended and contractors whose contracts had ended.

Recommendation

MWRA should develop a written policy that includes monitoring controls and a 24–business hour timeframe to ensure that the SPOC informs the MIS Department about MWRA employees whose employment has ended and contractors whose contracts have ended. MWRA should also train its employees on how to implement and follow this policy.

Auditee's Response

> *MWRA formalized* MWRA Information Security Policy for Access Control – Administrator, ADM.35 *on August 25, 2022 that addresses this finding. An additional Contractor Policy is also in draft that will specifically provide additional detail to address contractor physical access to MWRA facilities and access to the MWRA network as necessary. Appropriate staff will be trained on both policies to ensure that access is revoked in a timely manner for both employees and contractors.*

Auditor's Reply

Based on its response, MWRA is taking measures to address our concerns on this matter.