

ANSI/AWWA G430-24

(Revision of ANSI/AWWA G430-14(R20))

AWWA Management Standard

Security Practices for Operation and Management

Effective date: Aug. 1, 2024.

First edition approved by Board of Directors Jan. 25, 2009.

This edition approved Jan. 11, 2024.

Approved by American National Standards Institute Feb. 26, 2024.

Designation by the U.S. Department of Homeland Security SAFETY Act on Dec. 9, 2022.



AWWA Management Standard

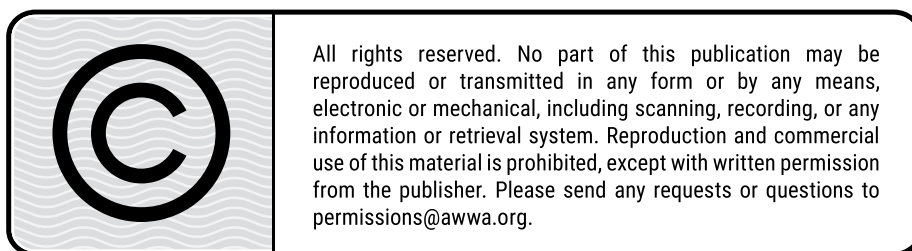
This document is an American Water Works Association (AWWA) management standard. It is not a specification. AWWA management standards describe consensus requirements for utility management practices. The use of AWWA management standards is entirely voluntary. This standard does not supersede or take precedence over or displace any applicable law, regulation, or code of any governmental authority. AWWA management standards are intended to represent a consensus of the water industry of requirements and practices that utilities should strive to achieve. When AWWA revises or withdraws this standard, an official notice of action will be placed in the Official Notice section of *Journal AWWA*. The action becomes effective on the first day of the month following the month of *Journal AWWA* publication of the official notice.

Note that this Standard was originally developed to incorporate the results of the NDWAC Report to USEPA on the “elements of an active and effective security program” for water-sector utilities. Following publication, this Standard was granted SAFETY Act designation as a Qualified Anti-Terrorism Technology. Although this Standard is voluntary, the prescriptive requirements included in the Standard (those expressed as “shall”) represent the minimum requirements that a utility must achieve to qualify for the SAFETY Act liability protections.

American National Standard

An American National Standard implies a consensus of those substantially concerned with its scope and provisions. An American National Standard is intended as a guide to aid the manufacturer, the consumer, and the general public. The existence of an American National Standard does not in any respect preclude anyone, whether that person has approved the standard or not, from manufacturing, marketing, purchasing, or using products, processes, or procedures not conforming to the standard. American National Standards are subject to periodic review, and users are cautioned to obtain the latest editions. Producers of goods made in conformity with an American National Standard are encouraged to state on their own responsibility in advertising and promotional materials or on tags or labels that the goods are produced in conformity with particular American National Standards.

CAUTION NOTICE: The American National Standards Institute (ANSI) approval date on the front cover of this standard indicates completion of the ANSI approval process. This American National Standard may be revised or withdrawn at any time. ANSI procedures require that action be taken to reaffirm, revise, or withdraw this standard no later than five years from the date of ANSI approval. Purchasers of American National Standards may receive current information on all standards by calling or writing the American National Standards Institute, 25 West 43rd Street, Fourth Floor, New York, NY 10036; (212) 642-4900, or e-mailing info@ansi.org.



ISBN-13, print: 978-1-64717-182-7

ISBN-13, electronic: 978-1-61300-709-9

DOI: <http://dx.doi.org/10.12999/AWWA.G430.24>

All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including scanning, recording, or any information or retrieval system. Reproduction and commercial use of this material is prohibited, except with written permission from the publisher.

Copyright © 2024 by American Water Works Association
Printed in USA

Committee Personnel

The AWWA Standards Committee on Security Practices for Operation and Management, which reviewed and approved this standard, had the following personnel at the time of approval:

Andrew Ohrt, *Chair*

Consumer Members

C. Herndon, Herndon Solutions Group, Las Vegas, Nev.

I. Jones, Alexandria, Va.

J.W. McLaughlin, Highfill, Mint Hill, N.C.

A. Ohrt, West Yost Associates, Duluth, Minn.

K. Owens, Control Cyber, Inc., Pullman, Wash.

C.R. Sapp, Arcadis, Virginia Beach, Va.

L.P. Warren, Launch! Consulting Inc., Charlottesville, Va.

Management Interest Members

C.L. Bowen, Pleasant Hill, Calif.

T.A. Kelly (*liaison, nonvoting*), Standards Council Liaison, Martinsburg, W.Va.

K. Morley, AWWA, Washington, D.C.

E.S. Ralph (*liaison, nonvoting*), Standards Engineer Liaison, AWWA, Denver, Colo.

User Members

R. Axtell, City of Sacramento, Folsom, Calif.

J. Hines, Las Vegas Valley Water District, Las Vegas, Nev.

M.I. Inyang, Massachusetts Water Resources Authority, Southborough, Mass.

Mike Stuhr, Chiloquin, Ore.

J. Taussig, Denver Water, Denver, Colo.

This page intentionally blank.

Contents

All AWWA standards follow the general format indicated subsequently. Some variations from this format may be found in a particular standard.

SEC.	PAGE	SEC.	PAGE
<i>Foreword</i>		4.4	Up-to-Date Assessment of Risk 8
I	Introduction..... vii	4.5	Resources Dedicated to Security and Security Implementation Priorities..... 9
I.A	Background..... vii	4.6	Access Control and Intrusion Detection 9
I.B	History viii	4.7	Contamination Detection, Monitoring, and Surveillance 12
I.C	Acceptance viii	4.8	Information Protection and Continuity 15
II	Special Issues viii	4.9	Design and Construction 17
II.A	Advisory Information on Application of Standards viii	4.10	Threat-Level–Based Protocols..... 18
II.B	Origination of Standard ix	4.11	Emergency Response and Recovery Plans and Business Continuity Plan..... 19
II.C	SAFETY Act Designation..... ix	4.12	Internal and External Communication..... 20
III	Use of This Standard ix	4.13	Partnerships..... 21
III.A	Options and Alternatives..... ix	5	Verification
III.B	Modification to Standard ix	5.1	Documentation Required..... 22
IV	Major Revisions..... ix	5.2	Human Resources 25
V	Comments x	5.3	Equipment 25
<i>Standard</i>		6	Delivery..... 25
1	General	<i>Appendixes</i>	
1.1	Scope..... 1	A	Resources 27
1.2	Purpose 1	B	Bibliography..... 39
1.3	Application..... 1	<i>Table</i>	
2	References 1	1	Supporting Documentation Required by this Standard by Section 21
3	Definitions 2	 Documents Document Sharing Hub	
4	Requirements		
4.1	Explicit Commitment to Security.... 6		
4.2	Security Culture 7		
4.3	Defined Security Roles and Employee Expectations..... 7		

This page intentionally blank.

Foreword

This foreword is for information only and is not a part of ANSI/AWWA G430.*

I. Introduction

I.A. *Background.* The AWWA Management Standards Program is designed to serve water, wastewater, and reuse utilities and their customers, owners, service providers, and government regulators. The standards developed under the program are intended to improve a utility's overall operation and service. Among these standards is this effort to establish formal management and operational guidelines. These guidelines identify appropriate practices, procedures, and behaviors—the implementation of which will provide effective and efficient utility operations and contribute to the protection of public health, public safety, and the environment.

AWWA's standards process has been used for more than 100 years to produce American National Standards Institute (ANSI)-recognized standards for materials and processes that are used by the water sector. These standards are recognized worldwide and have been adopted by many utilities and organizations. Likewise, this management standard is developed using the same ANSI-recognized formal process. Volunteer standards committees establish standard practices in a uniform and appropriate format.

Formal standards committees have been and continue to be formed to address the individual standard practices for the diverse areas of the water sector. A formal standards committee was created in 2007 to develop a standard for security. This standard is the outcome of the Security Practices for Operation and Management Committee.

The Utility Management G-Series Standards were developed to assist utilities with identifying and implementing applicable best management practices. To further enhance the use of the Standards, the AWWA Utility Quality Management Committee developed both self-assessment and peer-review programs to assist utilities that choose to meet performance criteria contained within the Standards. The Committee developed a framework for the stringent expectations of all Utility Management Standards, as follows:

- Utility Management Standards are voluntary, and their intent is to provide guidance toward best management practices.
- Requirements set forth in the Standards describe best practices that are achievable but not necessarily the best of class.

* American National Standards Institute, 25 West 43rd Street, Fourth Floor, New York, NY 10018

- The language used in the Standards should avoid requirements related to numeric values and words such as “shall” or “must” in areas that describe or could be considered in exceedance of existing local and/or federal regulations.

I.B. *History.* The first edition of this standard was approved by the AWWA Board of Directors on Jan. 25, 2009. The second edition was approved on June 8, 2014, and reaffirmed on Oct. 26, 2020. This edition was approved on Jan. 11, 2024.

I.C. *Acceptance.* No applicable information for this standard.

II. **Special Issues.**

II.A. *Advisory Information on Application of Standards.* This standard includes only those requirements that are limited exclusively to security practices for operation and management of a drinking water, wastewater, or reuse system. Separate standards will cover utility programs such as distribution system operation and management, emergency preparedness, financial management, water collection and treatment, source water protection, communication and customer relations, and business systems.

The America’s Water Infrastructure Act (AWIA) of 2018 (PL 115-270) requires community water systems serving a population of more than 3,300 to prepare a risk and resilience assessment and emergency response plan every five years. The risk and resilience assessment must consider threats from both malevolent acts and natural hazards that could affect the mission of the utility due to physical or cyber incidents. The findings of the risk and resilience assessment must then be used to inform the development of an emergency response plan that considers plans and procedures that can be implemented to “obviate or significantly lessen the impact” on the health, safety, and supply of drinking water from malevolent acts or natural hazards. The G430 standard provides the necessary framework to support the risk and resilience assessment and emergency response plan, including consideration of actions that reduce risk or enhance resilience as called for in AWIA. Application of the G430 standard is enhanced when implemented with complementary standards and resources, including the following:

- ANSI/AWWA J100—Risk and Resilience Management of Water and Wastewater Systems
- ANSI/AWWA G440—Emergency Preparedness Practices
- AWWA M19—Emergency Planning for Water and Wastewater Utilities
- AWWA Water Sector Resource Typing Guidance
- ANSI/AWWA G300—Source Water Protection
- AWWA Water Sector Cybersecurity Risk Management Guidance and Assessment Tool

II.B. *Origination of Standard.* This standard originates from recommendations prepared by the US Environmental Protection Agency (USEPA)'s National Drinking Water Advisory Council[†] (NDWAC) on water security practices, incentives, and measures, dated June 2005. A subsequent workgroup was convened in February 2007 by the Critical Infrastructure Partnership Advisory Council[‡] (CIPAC) to develop a national performance measurement system and revise the NDWAC recommendations to track with the Water Sector-Specific Plan (Water SSP), which is also described in Appendix A. Both sets of recommendations have informed the development of this standard.

II.C. *Support Anti-terrorism by Fostering Effective Technologies (SAFETY) Act Designation.* The ANSI/AWWA standards G430 and J100 have been awarded SAFETY Act designation by the US Department of Homeland Security. The designation carries important liability protection for the association and for utilities that properly implement these standards.

The SAFETY Act of 2002 was enacted by Congress in the wake of the terrorist attacks on Sept. 11, 2001. The SAFETY Act was created in part because of the extraordinarily large liability entities might face if a terrorist attack occurs despite deployment of anti-terrorism security measures already in place. Congress designed the SAFETY Act as an incentive for the creation and deployment of technologies and services with anti-terrorism capabilities. Under the SAFETY Act designation, both the entity that creates the anti-terrorism security measure and the entity that deploys the anti-terrorism measure are eligible for certain liability protections.

III. Use of This Standard. It is the responsibility of the user of an AWWA standard to determine that the products described in that standard are suitable for use in the particular application being considered.

III.A. *Options and Alternatives.* There is no applicable information in this section.

III.B. *Modification to Standard.* No applicable information for this section.

IV. Major Revisions. The major changes made to the standard in this revision include the following:

1. Added a paragraph on the background of the AWWA Utility Management G-Series standards to Sec. I.A. of the Foreword.

[†] National Drinking Water Advisory Council, Office of Ground Water and Drinking Water (4601), Ariel Rios Building, 1200 Pennsylvania Avenue, NW, Washington, DC 20460.

[‡] Critical Infrastructure Partnership Advisory Council, US Department of Homeland Security, Washington, DC 20528.

2. Added background on AWIA of 2018 to Sec. II.A of the Foreword.
3. Incorporated the AWIA of 2018 for Risk and Resilience Assessments and Emergency Response Plans requirements where applicable throughout standard.
4. Updated requirements for cybersecurity throughout.
5. Improved consistency with ANSI/AWWA J100 and ANSI/AWWA G440.
6. Updated Section 2 References.
7. In Section 3 Definitions, revised numerous definitions and added new definitions for AWIA, Risk and Resilience Assessment, and Risk and Resilience Management.
8. Added a new Sec. 4.7.7 Source water protection.
9. Added a new Sec. 4.9.1.3 Process control system design features.
10. Added a new Sec. 4.10.3 Monitor available threat information specific to enterprise systems.
11. Added a new Sec. 4.11.6 Response to enterprise systems.
12. Added new Secs. 4.13.1.3, 4.13.1.4, and 4.13.1.5 on establishing mutual aid relationships.
13. Updated Sec. A.2 Water Security Initiative Phase III with additional guidance.
14. Deleted Sec. A.4 Guidelines for Physical Security of Water and Wastewater/Stormwater Utilities.
15. Deleted Sec. A.5 Response Protocol Toolbox.
16. Added a new Sec. A.6 AWIA of 2018. Section 2013 Community Water System Risk and Resilience.

V. Comments. If you have any comments or questions about this standard, please contact AWWA Engineering and Technical Services at 303.794.7711; write to the department at 6666 West Quincy Avenue, Denver, CO 80235-3098; or e-mail at standards@awwa.org.



**American Water Works
Association**

Dedicated to the World's Most Vital Resource®

ANSI/AWWA G430-24
(Revision of ANSI/AWWA G430-14(R20))

AWWA Management Standard

Security Practices for Operation and Management

SECTION 1: GENERAL

Sec. 1.1 Scope

This standard covers the minimum requirements for a protective security program for a water, wastewater, or reuse utility.

Sec. 1.2 Purpose

The purpose of this standard is to define the minimum requirements for a protective security program for a water, wastewater, or reuse utility that will promote the protection of employee safety, public health, public safety, and public confidence.

Sec. 1.3 Application

This standard can be referenced in the evaluation of security practices. The stipulations of this standard apply when this document has been referenced and then only to the security practices of the utility.

SECTION 2: REFERENCES

This standard references the following documents. In their latest editions, or as specified, they form a part of this standard to the extent specified within

the standard, whether mentioned specifically or not. In any case of conflict, the requirements included within this standard shall prevail.

America's Water Infrastructure Act (AWIA) of 2018 (PL 115-270).

ANSI*/AWWA G440—Emergency Preparedness Practices.

ANSI/AWWA J100—Risk and Resilience Management of Water and Wastewater Systems.

AWWA *Process Control System Security Guidance for the Water Sector* (2017).

AWWA *Water Sector Cybersecurity Risk Management Guidance and Assessment Tool*.

AWWA *Water Sector Cybersecurity Risk Management Guidance for Small Systems*.

AWWA *Water Sector Resource Typing Guidance*.

Idaho National Laboratory[†] (INL)—Cyber-Informed Engineering Implementation Guide (2023).

National Electric Code Article 708^{*}.

Water Research Foundation[‡] (WRF)—*Business Continuity Planning for Water Utilities* (2008).

SECTION 3: DEFINITIONS

The following definitions shall apply in this standard.

1. *All hazards*: An approach for prevention, protection, preparedness, response, and recovery that addresses a full range of threats and hazards, including domestic terrorist attacks, natural and man-made disasters, accidental disruptions, and other emergencies.

2. *Asset*: An item of value or importance. In the context of critical water and wastewater infrastructure, an asset is something of importance or value that, if targeted, exploited, destroyed, or incapacitated, could result in serious interruption of the water supply to the community, illness and/or injury, death, economic damage to the community, financial damage to the owner of the asset, destruction of property, or environmental damage or could profoundly damage a utility's reputation, public confidence, or its ability to fulfill its mission(s). Assets may include physical elements (tangible property), subsystems, cyber elements

* American National Standards Institute, 25 West 43rd Street, 4th Floor, New York, NY 10036.

† Idaho National Laboratory, 1955 North Fremont Avenue, Idaho Falls, ID 83415.

‡ Water Research Foundation, 6666 West Quincy Avenue, Denver, CO 80235.

(information, process control, business and financial systems, and communication systems), and critical operational, technical, administrative, and managerial personnel.

- *Critical asset* is an asset whose absence or unavailability would significantly degrade the ability of a utility to carry out its mission or would have unacceptable financial, political, or physical consequences for the utility, the community, or the environment.

3. *AWIA*: America's Water Infrastructure Act (AWIA) of 2018 (PL 115-270). Additional information on AWIA can be found in Appendix A, Sec. A.6.

4. *Business continuity plan (BCP)*: A plan designed to maintain essential business functions and preserve the utility's ability to perform its mission or function during an incident and recovery. For example, a BCP should be designed to preserve the utility's ability to acquire and pay for essential supplies, personnel, components, or services; to receive funds; and to maintain a record of all transactions for subsequent accounting, billing, or reimbursement.

5. *Consequence*: The immediate, short-term, and long-term effects of a malevolent attack or natural, technological, or human-caused hazard. These effects include losses suffered by the owner of the asset and by the community served by that asset. They include human and property losses, environmental damages, and lifeline interruptions.

6. *Incident*: An occurrence (natural or human caused) that requires a response to protect life, property, continued service, the environment, or customer confidence. Incidents are unplanned and may include major disasters, emergencies, terrorist attacks, terrorist threats, civil unrest, wildfires, floods, hazardous material spills, nuclear accidents, earthquakes, hurricanes, tornadoes, tropical storms, tsunamis, public health and medical emergencies, and other occurrences requiring an emergency response.

7. *Incident command system (ICS)*: A standardized on-scene, all-hazards incident management concept that allows its users to adopt an integrated organizational structure to match the complexities and demands of single or multiple incidents without being hindered by jurisdictional boundaries. ICS is a scalable response to an emergency of any magnitude and provides a common framework within which responders from multiple agencies can work together.

8. *InfraGard*: InfraGard is an information-sharing and analysis effort serving the interests and combining the knowledge bases of a wide range of members. At its most basic level, InfraGard is a partnership between the Federal

Bureau of Investigation* (FBI) and the private sector. InfraGard is an association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States.

9. *Intrusion detection system (IDS)*: Intrusion detection for enterprise systems, supervisory control and data acquisition (SCADA), and process control systems is not a single product or a single piece of technology, even though commercial systems are available. Instead, intrusion detection is a comprehensive set of tools and processes providing network monitoring that can give an administrator a complete picture of how the network is being used. Implementing a variety of these tools helps to create a defense-in-depth architecture that can be more effective in identifying attacker activities and using the tools in a manner that can be preventive. Additional information on securing enterprise systems, process control systems, and SCADA systems can be found in Appendix A.

10. *National Incident Management System (NIMS)*: NIMS was developed by the US Department of Homeland Security (DHS) in response to Homeland Presidential Decision Directive 5 (HSPD-5) so that responders from different jurisdictions and disciplines can work together to better respond to natural disasters and emergencies, including acts of terrorism. NIMS benefits include a unified approach to incident management, standard command, and management structures. NIMS emphasizes preparedness, mutual aid, and resource management. NIMS uses the ICS, defined previously.

11. *National Infrastructure Protection Plan (NIPP)*: The NIPP is a strategy developed by the US DHS in response to HSPD-7 (since superseded by Presidential Decision Directive 21) that sets forth a comprehensive risk-management framework and clearly defines critical infrastructure protection roles and responsibilities for the DHS; federal sector risk-management agencies (SRMAs); and other federal, state, local, tribal, and private sector partners. The NIPP outlines the approach used to establish national priorities, goals, and requirements for critical infrastructure protection to support application of funding and resources in the most effective manner. For the water sector, the SRMA is the US Environmental Protection Agency (USEPA).

12. *Physical hardening*: A process designed to deter and/or help mitigate physical damage, service disruption, or other serious consequences of an attack

* FBI Headquarters 935 Pennsylvania Avenue, NW, Washington, D.C. 20535.

by making the facility harder to attack, delaying entry until responders arrive, or reducing the effect that an attack may have.

13. *Preparedness:* A continuous cycle of planning, organizing, training, equipping, exercising, and evaluating for emergency situations and taking corrective action in an effort to ensure effective coordination during the incident response and recovery, including continuity of operations plans, continuity of government plans, and preparation of resources for rapid restoration of function.

14. *Risk:* A function of the following: (1) consequences; (2) hazard frequency or threat likelihood; and (3) vulnerability, which, with point estimates, is the product of these three terms. It is the expected value of the consequences of an initiating event weighted by the likelihood of the event's occurrence and the likelihood that the event will result in the consequences, given that it occurs. Risk is based on identified events or event scenarios.

15. *Risk and Resilience Assessment:* To comply with AWIA, a Risk and Resilience Assessment shall include an assessment of the following:

- the risk to the system from malevolent acts and natural hazards;
- 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) that are used by the system;
- the monitoring practices of the system;
- the financial infrastructure of the system;
- the use, storage, or handling of various chemicals by the system; and
- the operation and maintenance of the system.

The assessment may include an evaluation of capital and operational needs for risk and resilience management for the system.

16. *Risk and Resilience Management:* A deliberate process of deciding whether actions are needed to reduce risk, improve resilience, or both and, if so, which options are most effective and efficient. If risk reduction or resilience enhancement is needed, decide on and implement one or a portfolio of options (e.g., establishing or improving security countermeasures, designing in consequence mitigation, building in redundancy, entering into mutual aid pacts, creating emergency response plans, or training and exercises in business continuity). The goal is to achieve an acceptable level of risk and resilience, relative to human casualties, service continuity, and financial effects on the utility and effects on

community well-being, at an acceptable cost to the utility and community. The ANSI/AWWA J100-21 standard provides a structured approach for a utility to reduce risk and improve resilience.

17. *Security plan:* A comprehensive plan, developed by the utility, that includes its security goals, objectives, strategies, policy or policies, and procedures. The security plan should coordinate closely with the utility's emergency preparedness and response plan, business continuity plan, and cybersecurity response plan.

18. *Vulnerability:* An inherent state of a system (e.g., physical, technical, organizational, cultural) that can be exploited by an adversary or affected by a natural hazard to cause harm or damage.

19. *Water sector:* The NIPP defines the water sector as both drinking water and wastewater utilities. For the purpose of this standard, this definition will expressly include water reclamation or reuse facilities.

20. *Water Sector Information Sharing and Analysis Center[†] (WaterISAC):* WaterISAC is a highly secure, subscription-based Internet portal that provides a source for sensitive security information and alerts to help the drinking water and wastewater community protect consumers and the environment.

SECTION 4: REQUIREMENTS

This standard is intended to apply to water, wastewater, or reuse utilities, regardless of size, location, ownership, or regulatory status. This standard builds on the long-standing practice among utilities of using a multiple-barrier approach for the protection of public health, public safety, and the environment. The requirements of this standard are designed to support a protective utility-specific security program that will result in consistent and measurable outcomes.

Sec. 4.1 Explicit Commitment to Security

4.1.1 *Explicit and visible commitment of senior leadership to security.* The utility shall establish an explicit, visible, easily communicated, and enterprise-wide commitment to security. This shall be represented by the development of security policies, procedures, and plans implemented as part of daily operations visible to employees and customers.

4.1.1.1 Periodic review and update of security plan, policies, or documents. The utility shall establish and maintain a schedule for periodic review of its security

[†] WaterISAC, 1620 I Street, NW, Suite 500, Washington, DC 20006.