

DRINKING WATER SYSTEM SECURITY & RESILIENCE STANDARDS

MICHIGAN WATER SECURITY SUMMIT
June 4, 2013

Clyde Dugan

THEME

UTILIZING A SUITE OF STANDARDS TO
ENHANCE YOUR SYSTEM'S SECURITY
AND RESILIENCE FOR ALL HAZARDS.

NATIONAL INFRASTRUCTURE PROTECTION PLAN 2009 (PREFACE)

Risk in the 21st century results from a complex mix of manmade and naturally occurring threats and hazards, including terrorist attacks, accidents, natural disasters, and other emergencies. Within this context, our critical infrastructure and key resources (CIKR) may be directly exposed to the event themselves or indirectly exposed as a result of the dependencies and interdependencies among CIKR.

PPD-21 (February 12, 2013)

- Presidential Policy Directive on Critical Infrastructure Security and Resilience
- Advances a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure
- The owner is in the best position to manage risks in their operations and to their assets and develop strategies to make them more secure and resilient against physical and cyber threats

AWWA STANDARDS

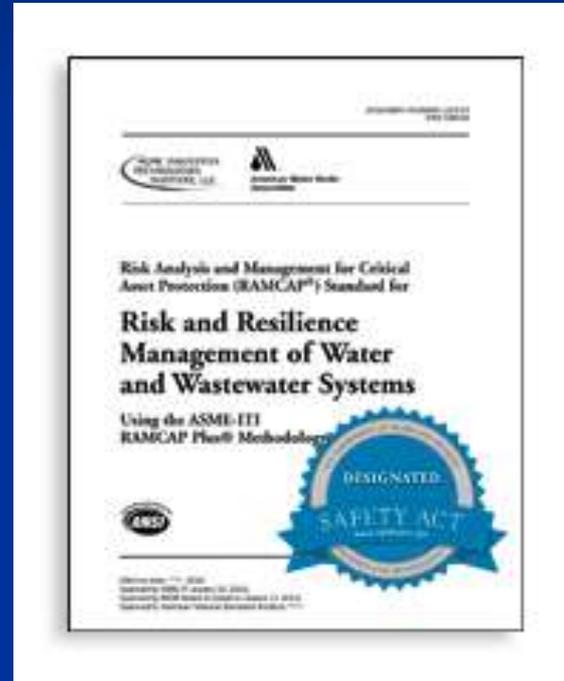
To assist utilities in meeting their responsibilities, AWWA has developed these standards:

- AWWA G430-09; Security Practices for Operation and Management
- AWWA J100-10; Risk and Resilience Management for Water and Wastewater Systems
- AWWA G440-11; Emergency Preparedness Practices

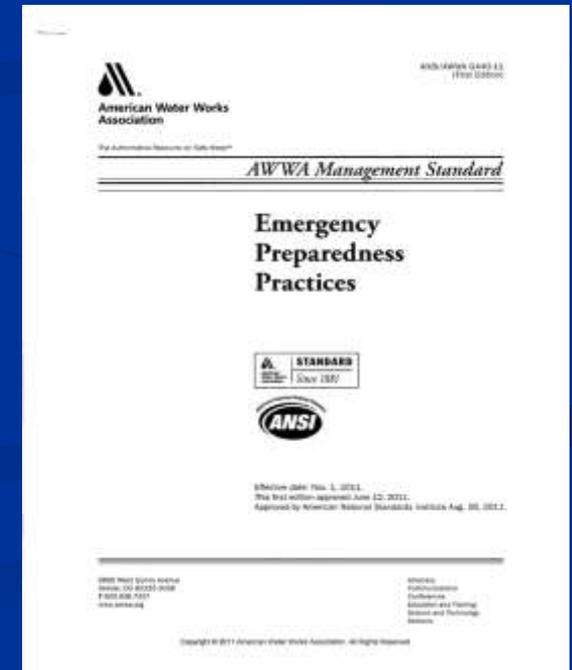
AWWA



G430-09



J100-10



G440-11

STANDARDS

SAFETY ACT DESIGNATION

- The Support Anti-terrorism by Fostering Effective Technologies Act of 2002 (“SAFETY Act”) was enacted by Congress in the wake of the terrorist attacks on September 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 qualified anti-terrorism technologies and services.

SAFETY ACT DESIGNATION

The American Water Works Association 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.

SAFETY ACT DESIGNATION

DHS has concluded that the proper utilization of either of these Standards will assist in effectively mitigating acts of terrorism from occurring at water facilities.

Stakeholders are also assured that, with proper use of the Standards, they are protected from third-party lawsuits should an act of terrorism occur involving a Standard-identified vulnerability.

DEFINITIONS

- The term "resilience" refers to the ability to adapt to changing conditions and withstand and rapidly recover from disruption due to emergencies.
- The term "all hazards" refers to 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.

Key Features of an Active and Effective Protective Program (USEPA)

- The Features originated as an outcome of a NDWAC Water Security Working Group in 2005 and have been updated to reflect the goals and objectives of the Sector Specific Plan for Water.
- The Features use terms like "protective" to describe activities that enhance resiliency and promote continuity of service, regardless of the exact type of hazard or adverse effect a utility might experience.
- The Key Features describe the basic elements of a "protective program" for owners/operators of utilities to consider as they develop utility-specific approaches. They address the physical, cyber, and human elements of prevention, detection, response, and recovery.

Key Features of an Active and Effective Protective Program (USEPA)

1. Integrate protective concepts into organizational culture, leadership, and daily operations
2. Identify and support protective program priorities, resources, and measures
3. Employ protocols for detection of contamination
4. Assess risks and review vulnerability assessments
5. Establish facility and information access controls
6. Incorporate resiliency concepts into physical infrastructure
7. Prepare, test and update emergency response, recovery and business continuity plans
8. Form partnerships with peers and interdependent sectors
9. Develop and implement internal and external communication strategies
10. Monitor incidents and threat level information

**AWWA STANDARD:
SECURITY PRACTICES FOR
OPERATION AND
MANAGEMENT**

ANSI/AWWA G430-09

AWWA STANDARD: SECURITY PRACTICES FOR OPERATION AND MANAGEMENT

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

AWWA STANDARD: SECURITY PRACTICES FOR OPERATION AND MANAGEMENT

- Applies to all water & wastewater utilities, irrespective of size, location, ownership, or regulatory status.
- Builds on the long-standing practice of utilizing a multiple barrier approach for the protection of public health and safety.
- Designed to support an active and effective utility-specific security program.
- If implemented, the Utility will realize consistent and measurable outcomes.

AWWA STANDARD: SECURITY PRACTICES FOR OPERATION AND MANAGEMENT

KEY ELEMENTS OF THE STANDARD:

- Explicit commitment to security

AWWA STANDARD: SECURITY PRACTICES FOR OPERATION AND MANAGEMENT

KEY ELEMENTS OF THE STANDARD:

- Explicit commitment to security
- Security culture

AWWA STANDARD: SECURITY PRACTICES FOR OPERATION AND MANAGEMENT

KEY ELEMENTS OF THE STANDARD:

- Explicit commitment to security
- Security culture
- Defined security roles and employee expectations

AWWA STANDARD: SECURITY PRACTICES FOR OPERATION AND MANAGEMENT

KEY ELEMENTS OF THE STANDARD:

- Explicit commitment to security
- Security culture
- Defined security roles and employee expectations
- Up-to-date assessment of vulnerability

AWWA STANDARD: SECURITY PRACTICES FOR OPERATION AND MANAGEMENT

KEY ELEMENTS OF THE STANDARD:

- Explicit commitment to security
- Security culture
- Defined security roles and employee expectations
- Up-to-date assessment of vulnerability
- Resources dedicated to security and security implementation priorities

AWWA STANDARD: SECURITY PRACTICES FOR OPERATION AND MANAGEMENT

KEY ELEMENTS OF THE STANDARD:

- Explicit commitment to security
- Security culture
- Defined security roles and employee expectations
- Up-to-date assessment of vulnerability
- Resources dedicated to security and security implementation priorities
- Access control and intrusion detection

AWWA STANDARD: SECURITY PRACTICES FOR OPERATION AND MANAGEMENT

KEY ELEMENTS OF THE STANDARD:

- Contamination detection, monitoring and surveillance

AWWA STANDARD: SECURITY PRACTICES FOR OPERATION AND MANAGEMENT

KEY ELEMENTS OF THE STANDARD:

- Contamination detection, monitoring and surveillance
- Information protection and continuity

AWWA STANDARD: SECURITY PRACTICES FOR OPERATION AND MANAGEMENT

KEY ELEMENTS OF THE STANDARD:

- Contamination detection, monitoring and surveillance
- Information protection and continuity
- Threat level-based protocols

AWWA STANDARD: SECURITY PRACTICES FOR OPERATION AND MANAGEMENT

KEY ELEMENTS OF THE STANDARD:

- Contamination detection, monitoring and surveillance
- Information protection and continuity
- Threat level-based protocols
- Emergency response and recovery plans

AWWA STANDARD: SECURITY PRACTICES FOR OPERATION AND MANAGEMENT

KEY ELEMENTS OF THE STANDARD:

- Contamination detection, monitoring and surveillance
- Information protection and continuity
- Threat level-based protocols
- Emergency response and recovery plans
- Internal and external communications

AWWA STANDARD: SECURITY PRACTICES FOR OPERATION AND MANAGEMENT

KEY ELEMENTS OF THE STANDARD:

- Contamination detection, monitoring and surveillance
- Information protection and continuity
- Threat level-based protocols
- Emergency response and recovery plans
- Internal and external communications
- Partnerships

AWWA STANDARD: SECURITY PRACTICES FOR OPERATION AND MANAGEMENT

KEY ELEMENTS OF THE STANDARD:

- Explicit commitment to security
- Security culture
- Defined security roles and employee expectations
- Up-to-date assessment of vulnerability
- Resources dedicated to security and security implementation priorities
- Access control and intrusion detection
- Contamination detection, monitoring and surveillance
- Information protection and continuity
- Threat level-based protocols
- Emergency response and recovery plans
- Internal and external communications
- Partnerships

AWWA STANDARD: SECURITY PRACTICES FOR OPERATION AND MANAGEMENT

How Does It Work? Let's take an example:

- Explicit commitment to security
- Security culture
- Defined security roles and employee expectations
- Up-to-date assessment of vulnerability
- Resources dedicated to security and security implementation priorities
- Access control and intrusion detection

AWWA STANDARD: SECURITY PRACTICES FOR OPERATION AND MANAGEMENT

How Does It Work? Let's take an example:

- Explicit commitment to security
- Security culture
- Defined security roles and employee expectations
- Up-to-date assessment of vulnerability
- Resources dedicated to security and security implementation priorities
- **Access control and intrusion detection**

AWWA STANDARD: SECURITY PRACTICES FOR OPERATION AND MANAGEMENT

Under this heading, you'll find (8) activities that support this requirement:

1. Identify utility assets requiring access control
2. Establish and maintain physical control of access to identified critical assets
3. Implement annual inspections of identified critical assets
4. Establish and maintain a means of detecting and assessing intrusion
5. Establish and maintain procedures to control personnel access to identified critical assets
6. Establish and maintain a means of restricting authorization for access
7. Establish a protocol for employees or others that have been terminated, resigned or had a relevant change of status
8. Testing

AWWA STANDARD: SECURITY PRACTICES FOR OPERATION AND MANAGEMENT

Supporting information on how to accomplish this:

1. Identify utility assets requiring access control
2. Establish and maintain physical control of access to identified critical assets
3. Implement annual inspections of identified critical assets
4. Establish and maintain a means of detecting and assessing intrusion
5. Establish and maintain procedures to control personnel access to identified critical assets
6. Establish and maintain a means of restricting authorization for access
7. Establish a protocol for employees or others that have been terminated, resigned or had a relevant change of status
8. Testing

AWWA STANDARD: SECURITY PRACTICES FOR OPERATION AND MANAGEMENT

7. Establish a protocol for employees or others that have been terminated, resigned or had a relevant change of status.

The utility shall establish and maintain a protocol to recover keys, revise passwords and take other appropriate actions immediately upon termination, resignation or re-assignment of an employee or the relevant change of status of other personnel who have access to high-risk assets.

Other personnel may include vendors, consultants, contractors, public officials or others that had been granted appropriate access and are no longer performing a relevant function.

AWWA STANDARD: SECURITY PRACTICES FOR OPERATION AND MANAGEMENT

Verification:

Section 5 of the standard covers the documentation required of the utility to verify it has performed as required.

In this case:

Establish a protocol for employees or others that have been terminated, resigned or had a relevant change of status.

Documentation Required:

Documented procedures for review or revocation of security access rights for employees or others who have had a change-of-status.

AWWA STANDARD: SECURITY PRACTICES FOR OPERATION AND MANAGEMENT

Application of the requirements of this Standard will lead the utility to compliance with the requirements of the Key Features of an Active and Effective Protection Program and enhance resiliency.

G430 is currently being updated, so-as to stay current in this evolving environment.

ASME/AWWA STANDARD:

**RISK AND RESILIENCE
MANAGEMENT OF WATER
AND WASTEWATER SYSTEMS**

ANSI/ASME-ITI/AWWA J100-10

ASME/AWWA STANDARD: RISK AND RESILIENCE MANAGEMENT

The long title is:

Risk Analysis and Management for Critical Asset Protection (RAMCAP[®]) Standard for Risk and Resilience Management of Water and Wastewater Systems Using the ASME-ITI RAMCAP Plus[®] Methodology

ASME/AWWA STANDARD: RISK AND RESILIENCE MANAGEMENT

The RAMCAP[®] methodology was developed by ASME after 9/11/01 to establish a common framework for risk analysis within and across industry sectors.

There has been an evolution in the NIPP from an evaluation of terrorism only to an evaluation of risk from natural and man-made hazards; an all hazards approach.

This Standard uses the all hazards approach.

ASME/AWWA STANDARD: RISK AND RESILIENCE MANAGEMENT

The 2002 Bioterrorism Preparedness and Response Act required systems serving >3,300 to perform a vulnerability assessment. For the water sector, most utilities utilized either the RAM-W or the VSAT methodologies, and the focus was on terrorism-related design basis threats. Current versions of these products do not reflect all aspects of J100.

Breaking News; EPA has decided to upgrade VSAT 5.0 to be consistent with the J100 methodology. The new version will be available this fall.

ASME/AWWA STANDARD: RISK AND RESILIENCE MANAGEMENT

Based on the “Key Features”, G430 & G440 require utilities to update their vulnerability assessments every 5 years, or more frequently if conditions warrant.

This J100 Standard is and will be maintained to be consistent with the current all-sector RAMCAP[®] standard, and therefore provides utilities with a repeatable platform for these assessments.

ASME/AWWA STANDARD: RISK AND RESILIENCE MANAGEMENT

Using this standard, vulnerabilities and weaknesses are identified for;

- Man-made threats,
- Natural hazards,
- Dependencies,
- Proximity to hazardous sites

Methods to evaluate options for improving identified weaknesses are explored as a part of the Risk Management phase of the analysis.

ASME/AWWA STANDARD: RISK AND RESILIENCE MANAGEMENT

J100 utilizes a 7-step Iterative Process:

1. Asset Characterization
2. Threat Characterization
3. Consequence Analysis
4. Vulnerability Assessment
5. Threat Analysis
6. Risk/Resilience Analysis
7. Risk/Resilience Management

ASME/AWWA STANDARD: RISK AND RESILIENCE MANAGEMENT

The analysis utilizes a “Worst Reasonable Case” assumption for evaluating consequences, so they are reasonable and credible and do not combine unlikely coincidences.

Once the utility understands its risks, then risk management is a means of reducing that risk to an acceptable level at a reasonable cost.

ASME/AWWA STANDARD: RISK AND RESILIENCE MANAGEMENT

AWWA On-Line Course:

- EL110 - J100 RAMCAP® Risk and Resilience Management of Water and Wastewater Systems E-Learning Course
- Course Length: 20 Hours / 2 CEUs
- Member Price: \$695.00, including a copy of Standard.
- MDEQ OTCU list the course as approved for 2.0 CEUs Water and Wastewater – Managerial.

AWWA STANDARD:

EMERGENCY

PREPAREDNESS PRACTICES

ANSI/AWWA G440-11

AWWA STANDARD: EMERGENCY PREPAREDNESS PRACTICES

The purpose of this standard is to define the minimum emergency preparedness requirements for water, wastewater or reuse facilities to respond to emergencies and restore normal operations...

AWWA STANDARD: EMERGENCY PREPAREDNESS PRACTICES

KEY ELEMENTS OF THE STANDARD:

- Explicit commitment to emergency preparedness
- Preparedness culture
- Defined emergency preparedness roles and expectations
- Risk Assessment
- Preparedness Plans
- Internal and External Communications
- Training
- Partnerships

AWWA STANDARD: EMERGENCY PREPAREDNESS PRACTICES

How Does It Work?

As one of the Management-Series Standards, this G440 is designed the same way as G430;

Each primary elements is subdivided into specific requirements that support it, and the necessary documentation is defined to verify compliance.

G440 Provides excellent information and guidance for utilities in establishing an emergency preparedness plan and culture.

SUMMARY

Security requirements for critical infrastructure in the United States in general and in the Water Sector specifically, are evolving.

We've seen the evolution from terrorism to all-hazards and from facility-based security to resilience.

We've also seen adaptations in the nature of man-made hazards; currently the emphasis is on cyber attacks.

SUMMARY

Using the tools and techniques identified, coupled with a frequent review of the utility's vulnerabilities and preparedness plans, will allow utilities to adapt to these and future evolutionary changes.

Doing our part will also support other initiatives aimed at promoting a community-wide resiliency.

ADDITIONAL SUPPORTING MATERIALS

- AWWA Manual M9; Emergency Planning for Water Utilities
- ANSI/ASCE Standard 56-10; Guidelines for the Physical Security of Water Utilities
- ANSI/ASCE Standard 57-10; Guidelines for the Physical Security of Wastewater / Stormwater Utilities
- US EPA; Key Features of an Active and Effective Protective Program