All-Hazards Approach to Water Sector Security & Preparedness

ANSI-HSSP
Arlington, VA
November 9, 2011

Security and Resilience

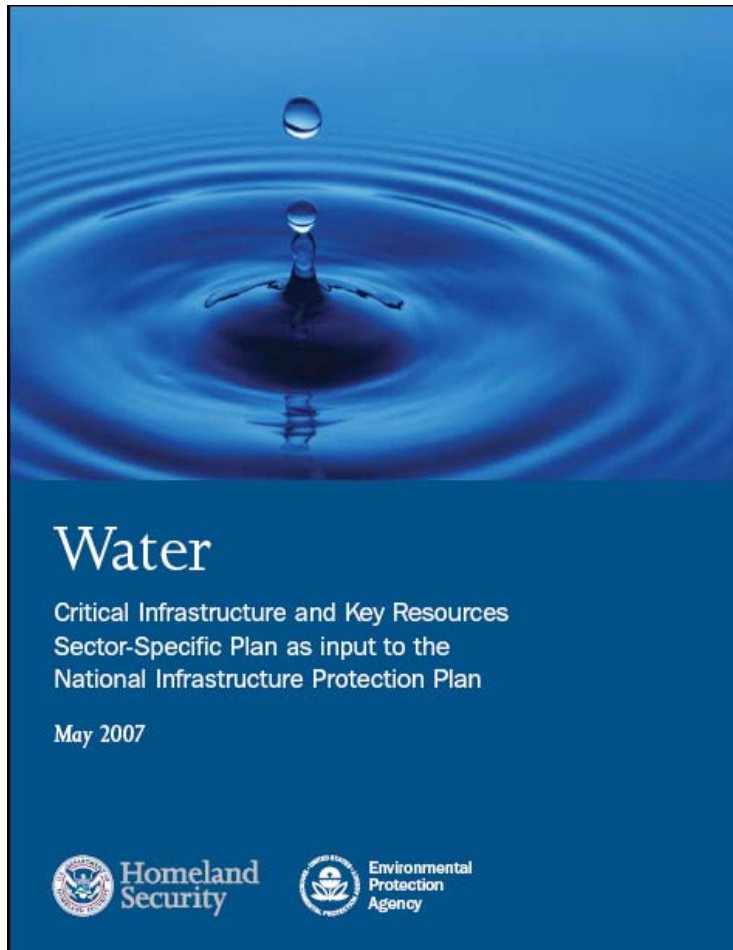Guns/Gates/Guards

vs

Response, Recovery, Resilience

Key Points in Time

- December 7, 1941 – Pearl Harbor

- April 19, 1995 – Oklahoma City

- December 31, 1999 – Y2K

- September 11, 2001 – WTC, Pentagon, PA

- August 29, 2005 – Hurricane Katrina

The Water Sector Vision

Water

Critical Infrastructure and Key Resources
Sector-Specific Plan as input to the
National Infrastructure Protection Plan

May 2007

Homeland Security

Environmental Protection Agency

A __secure and resilient__ drinking water and wastewater infrastructure that provides clean and safe water as an integral part of daily life. This Vision assures the economic vitality of and public confidence in the nation's drinking water and wastewater through a __layered defense of effective preparedness and security practices__ in the sector.

WATER SECTOR COORDINATING COUNCIL

- Established in 2004 under the HSPD-7 National Infrastructure Protection Plan framework for partnership with CI/KR.

- The WSCC serves as a policy, strategy and coordinating mechanism that recommends actions to reduce and eliminate significant homeland security vulnerabilities to the water sector through interactions with the Federal Government and other critical infrastructure sectors.

SSP Goals

1. Sustain protection of public health and the environment.

2. Recognize and reduce risks in the water sector.

3. Maintain a resilient infrastructure.

4. Increase communication, outreach, and public confidence.
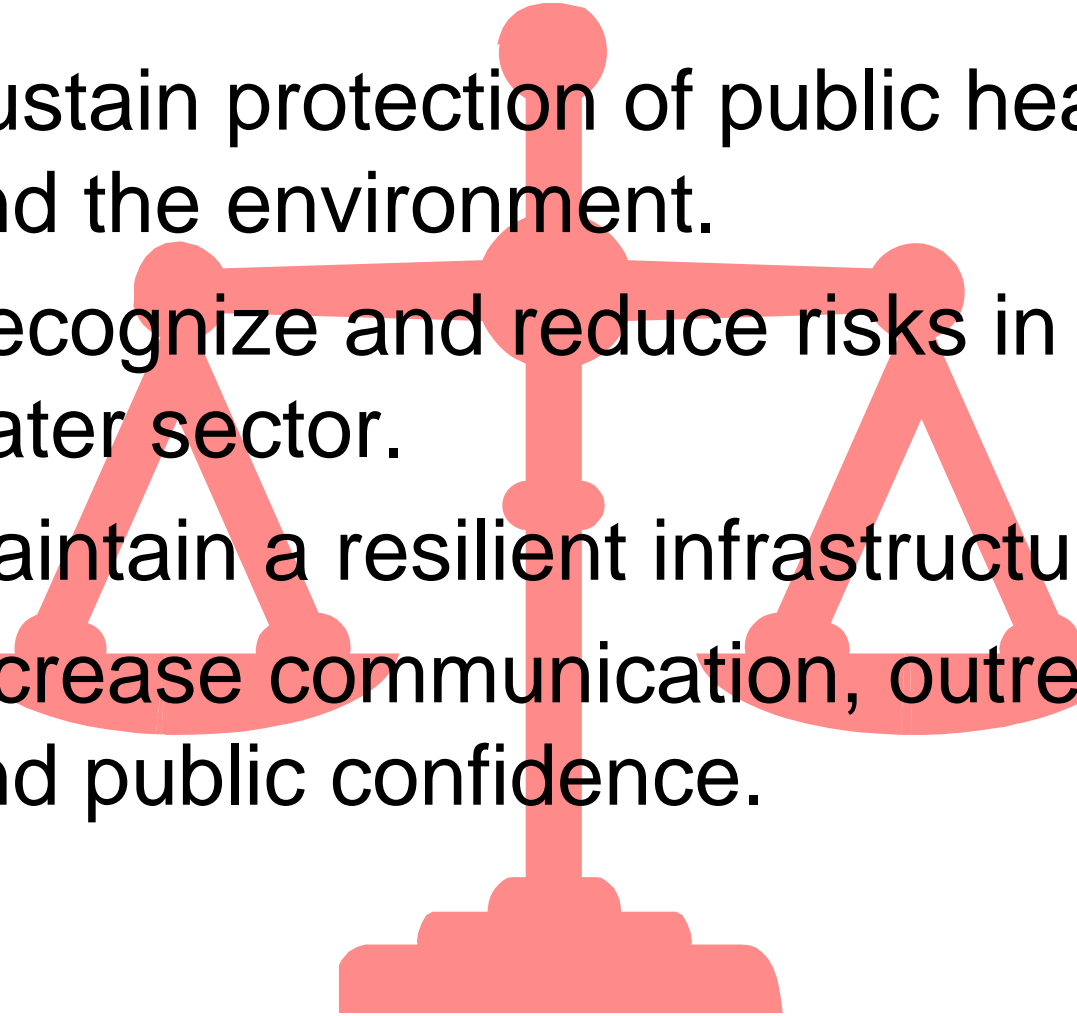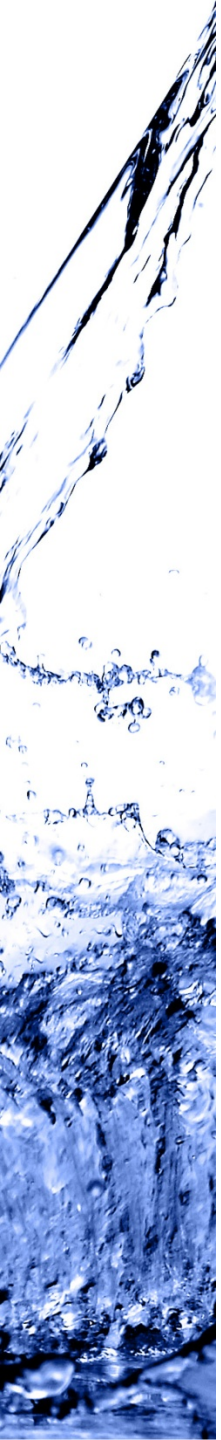
Standards & Guidance

1. ANSI/AWWA G430-09: Security Practices for Operations and Management

2. ANSI/ASME-ITI/AWWA J100-10 Risk Analysis and Management for Critical Asset Protection (RAMCAP) Standard for Risk and Resilience Management of Water and Wastewater Systems

3. AWWA G440: Emergency Preparedness Practices (pending)

4. M19: Emergency Planning for Water Utilities

ANSI/AWWA G430-09:
Security Practices for Operations and Management

Purpose: This standard defines the minimum requirements for a protective security program for a water or wastewater utility that will promote the protection of employee safety, public health, public safety, and public confidence.

This standard builds on the long-standing practice amongst utilities of utilizing a multiple barrier approach for the protection of public health and safety.

ANSI/AWWA G430-09:
Security Practices for Operations and Management

Requirements:

a) Explicit Commitment to Security
b) Security Culture
c) Defined Security Roles and Employee Expectations
d) Up-To-Date Assessment of Risk (Vulnerability)
e) Resources Dedicated to Security and Security Implementation Priorities
f) Access Control and Intrusion Detection
g) Contamination, Detection, Monitoring and Surveillance
h) Information Protection and Continuity
i) Design and Construction
j) Threat Level-Based Protocols
k) Emergency Response and Recovery Plans and Business Continuity Plan
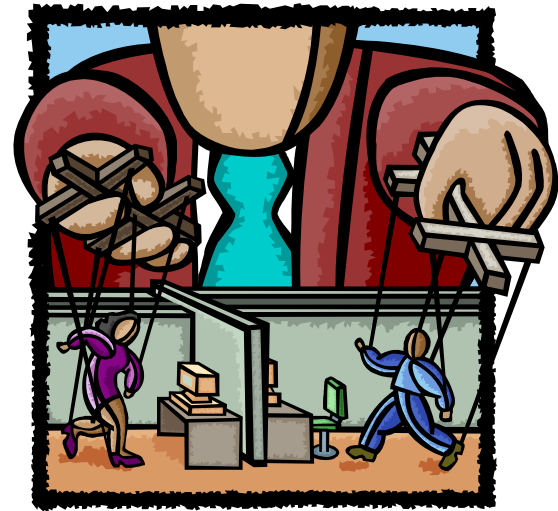l) Internal and External Communications
m) Partnerships
n) Verification

ANSI/AWWA G430-09:
Security Practices for Operations and Management

Requirements:

a) Explicit Commitment to Security
b) Security Culture
c) Defined Security Roles and Employee Expectations
d) Up-To-Date Assessment of Risk (Vulnerability)
e) Resources Dedicated to Security and Security Implementation Priorities
f) Access Control and Intrusion Detection
g) Contamination, Detection, Monitoring and Surveillance
h) Information Protection and Continuity
i) Design and Construction
j) Threat Level-Based Protocols
k) Emergency Response and Recovery Plans and Business Continuity Plan
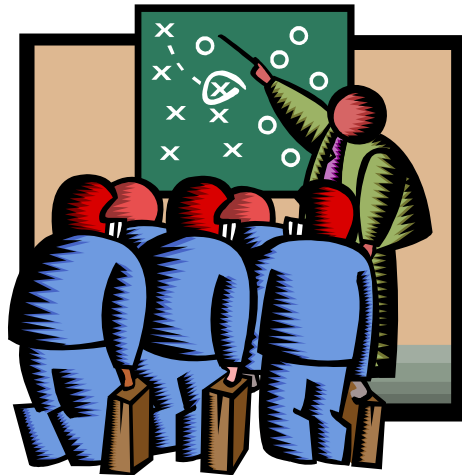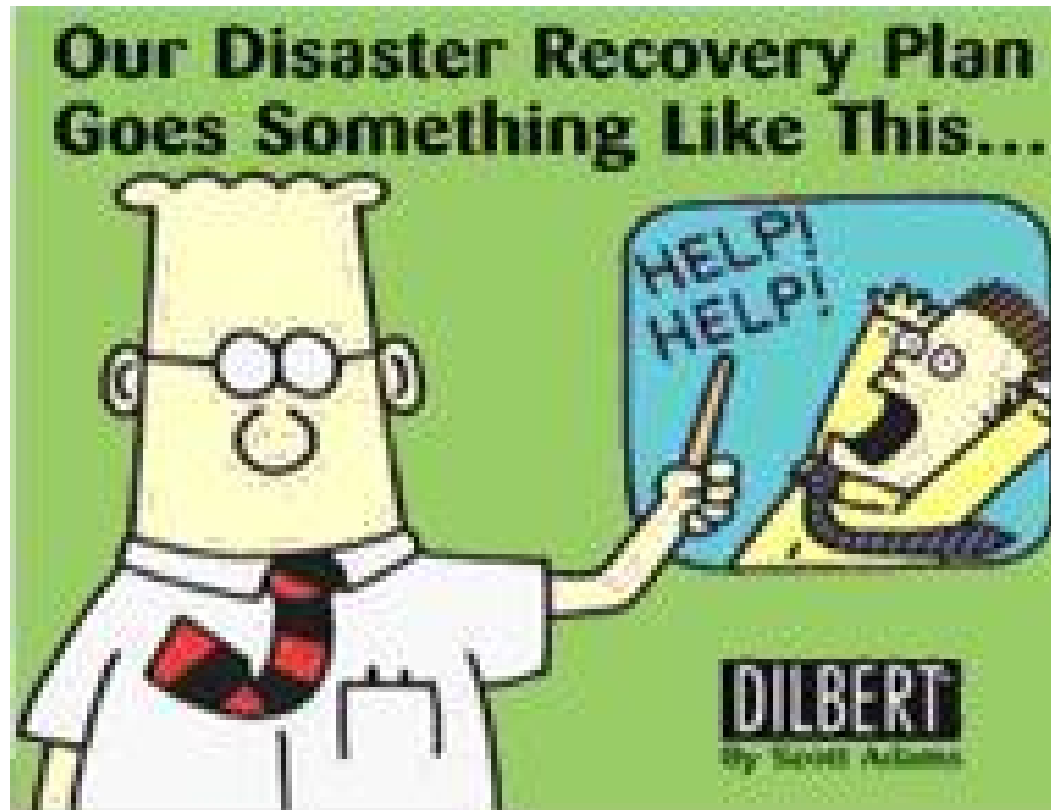l) Internal and External Communications
m) Partnerships
n) Verification
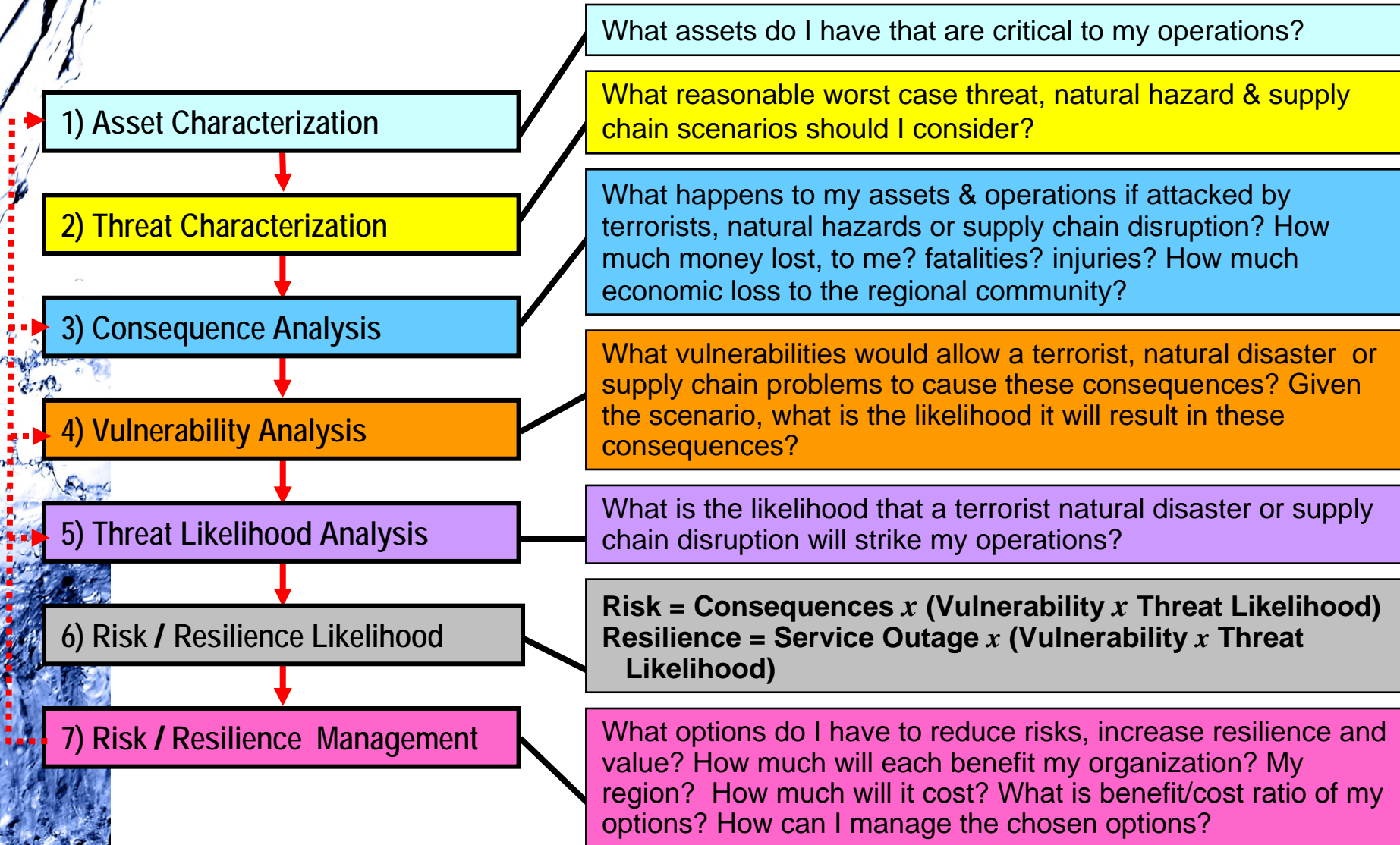
Where is Management?

Hopefully this is not the answer

ANSI/AWWA G430-09:
Security Practices for Operations and Management

Requirements:

a) Explicit Commitment to Security
b) Security Culture
c) Defined Security Roles and Employee Expectations
d) Up-To-Date Assessment of Risk (Vulnerability)
e) Resources Dedicated to Security and Security Implementation Priorities
f) Access Control and Intrusion Detection
g) Contamination, Detection, Monitoring and Surveillance
h) Information Protection and Continuity
i) Design and Construction
j) Threat Level-Based Protocols
k) Emergency Response and Recovery Plans and Business Continuity Plan
l) Internal and External Communications
m) Partnerships
n) Verification

The J100 RAMCAP Process

1) Asset Characterization

What assets do I have that are critical to my operations?

2) Threat Characterization

What reasonable worst case threat, natural hazard & supply chain scenarios should I consider?

3) Consequence Analysis

What happens to my assets & operations if attacked by terrorists, natural hazards or supply chain disruption? How much money lost, to me? fatalities? injuries? How much economic loss to the regional community?

4) Vulnerability Analysis

What vulnerabilities would allow a terrorist, natural disaster or supply chain problems to cause these consequences? Given the scenario, what is the likelihood it will result in these consequences?

5) Threat Likelihood Analysis

What is the likelihood that a terrorist natural disaster or supply chain disruption will strike my operations?

6) Risk / Resilience Likelihood

Risk = Consequences x (Vulnerability x Threat Likelihood)
Resilience = Service Outage x (Vulnerability x Threat Likelihood)

7) Risk / Resilience Management

What options do I have to reduce risks, increase resilience and value? How much will each benefit my organization? My region? How much will it cost? What is benefit/cost ratio of my options? How can I manage the chosen options?

ANSI/AWWA G430-09:
Security Practices for Operations and Management

Requirements:

a) Explicit Commitment to Security
b) Security Culture
c) Defined Security Roles and Employee Expectations
d) Up-To-Date Assessment of Risk (Vulnerability)
e) Resources Dedicated to Security and Security Implementation Priorities
f) Access Control and Intrusion Detection
g) Contamination, Detection, Monitoring and Surveillance
h) Information Protection and Continuity
i) Design and Construction
j) Threat Level-Based Protocols
k) Emergency Response and Recovery Plans and Business Continuity Plan
l) Internal and External Communications
m) Partnerships
n) Verification

AWWA G440: Emergency Preparedness Practices (ANSI designation pending)

Purpose: This standard defines the minimum requirements for emergency preparedness for a water or wastewater utility. Emergency preparedness practices include the development of an emergency response plan (hazard evaluation, hazard mitigation, response planning, and mutual aid agreements), the evaluation of the emergency response plan through exercises, and the revision of the emergency response plan after exercises.

ANSI/AWWA G440-11:
Emergency Preparedness Practices

Requirements:

4.1 Explicit Commitment to Emergency Preparedness

4.2 Preparedness Culture

4.3 Defined Preparedness Roles and Employee Expectations

4.3 Risk Assessment

4.4 Preparedness Plans

4.5 Internal and External Communications

4.6 Training

4.7 Partnerships

5.0 Verification

M19: Emergency Planning for Water Utilities

- Core Elements:
  - Hazard Summary
  - Vulnerability Assessment
  - Mitigation Actions
  - Preparedness Planning
  - Emergency Response, Recovery & Training

- Complements G430, J100, G440

Emergency Water Supply
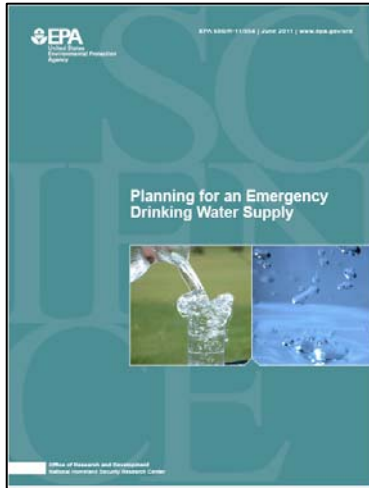
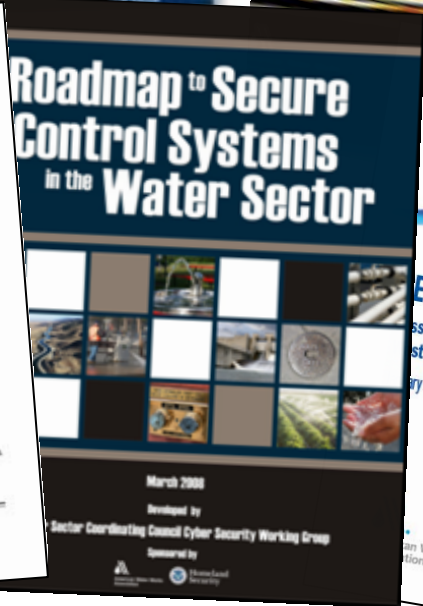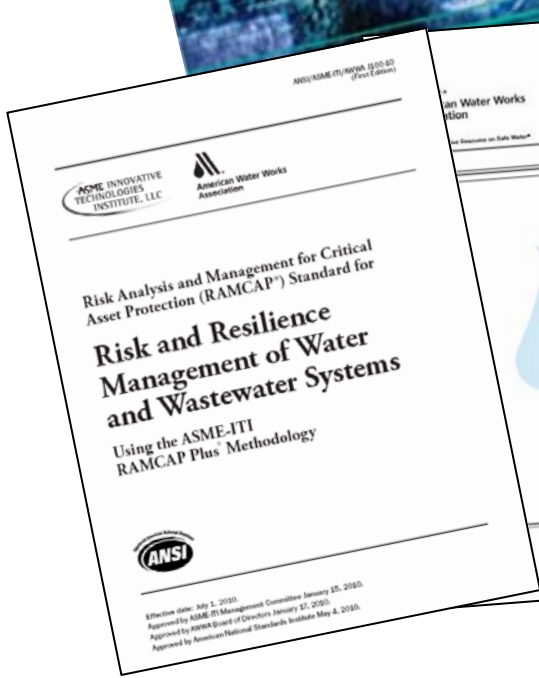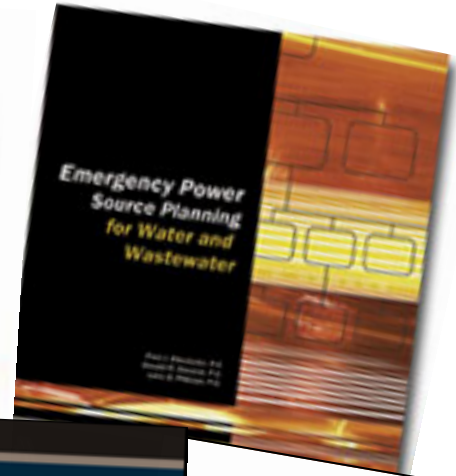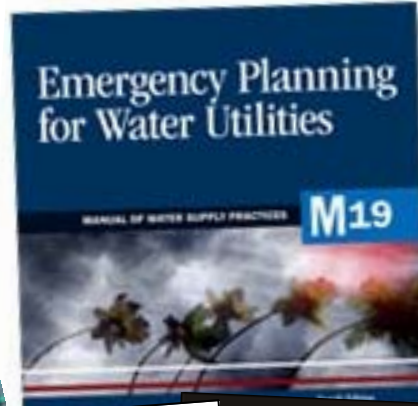**Planning for an Emergency Drinking Water Supply**

- EPA-NHSRC/AWWA collaboration
- Provide guidance for utility preparedness
- Clarify roles and responsibilities
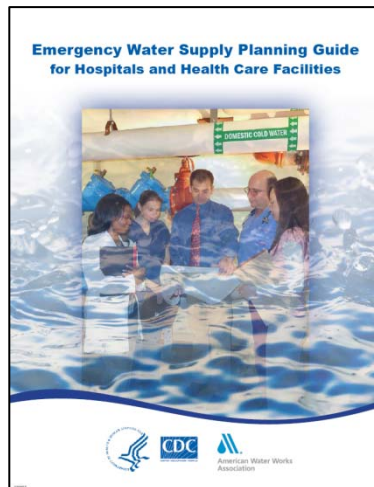
Emergency Water Supply Planning for Hospitals and Health Care Facilities

- CDC/AWWA collaboration
- Address gaps in Joint Commission standards

Additional Resources

Questions

Kevin M. Morley
Security & Preparedness Program Manager
AWWA – Government Affairs
1300 Eye Street, NW Suite 701W
Washington, DC 2005
202-628-8303 or kmorley@awwa.org

Advancing Security and Emergency Preparedness in the Water Sector