

University of Colorado
Colorado Springs


CS4950/5950
Homeland Security & Cybersecurity

Drinking Water Infrastructure

CS 4950/5950
Homeland Security &
Cybersecurity


Lesson 16
Drinking Water
Infrastructure

Rick White, Ph.D.
University of Colorado, Colorado
Springs



1
Esc

1

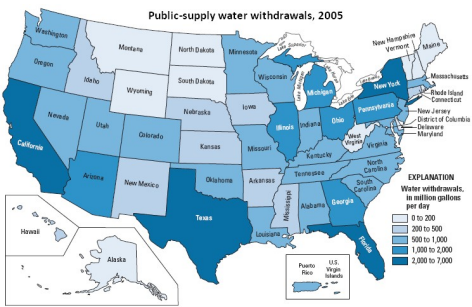


University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity


Drinking Water Infrastructure

The US water and wastewater sectors are comprised of approximately **55,000 public water systems** that serve drinking water to more than **300 million people** and approximately 16,500 publicly owned treatment facilities that treat wastewater for more than 227 million people and certain industries.



2
Esc

2




University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity


Drinking Water Infrastructure

The water and wastewater sectors are **regulated by the Environmental Protection Agency** under the 1974 Safe Drinking Water Act, 1972 Clean Water Act, and provisions of the 1970 Clean Air Act.



3 Esc

3

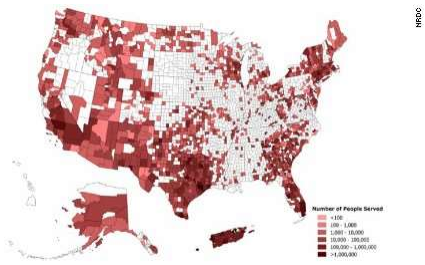


University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Drinking Water Infrastructure

- About 15% of drinking water and wastewater utilities located primarily in urban areas provide water services to more than 75% of the US population.
- Arguably, these systems present targets of opportunity for malicious attack.

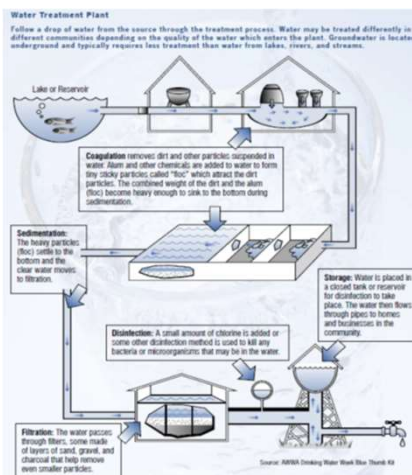


4 Esc

4

Drinking Water Infrastructure

- Cyber attacks targeting operating facilities, electronic control systems, and pumping stations could result in physical destruction and long term disruption to service.
- Water infrastructure system designers, managers, and operators have long made preparing for extreme events a standard practice.



5

Esc

5

Drinking Water Infrastructure

- Historically, though, their focus has been on natural events – major storms, blizzards, and earthquakes – some of which can be predicted hours before they occur.
- When considering the risk of manmade threats, operators generally focused on malicious acts of vandalism or theft by disgruntled employees or customers.
- 9/11 significantly broadened their concerns.



6

Esc

6



University of Colorado
Colorado Springs

CS4950/5950

Homeland Security & Cybersecurity

Drinking Water Infrastructure

As specified in PPD-21 and the 2013 National Infrastructure Protection Plan, the **EPA is the Sector-Specific Agency responsible for coordinating security measures with industry** represented by membership on the Water Sector Coordinating Council.

<https://www.whitehouse.gov/the-press-office/2013/02/12/2013-02-12-critical-infrastructure-security-and-resilience>

The White House
Office of the Press Secretary
For Immediate Release
February 12, 2013
Presidential Policy Directive -- Critical Infrastructure Security and Resilience
PRESIDENTIAL POLICY DIRECTIVE PPD-21
SUBJECT: Critical Infrastructure Security and Resilience
The Presidential Policy Directive (PPD) on Critical Infrastructure Security and Resilience advances a national unity of efforts to strengthen and maintain secure, functioning, and resilient critical infrastructure.
Background
The nation's critical infrastructure provides the essential services that underpin American society. Proactive and coordinated efforts are necessary to strengthen and maintain secure, functioning, and resilient critical infrastructure -- including assets, networks, and systems -- that are vital to public confidence and the nation's safety, prosperity, and well-being.
The nation's critical infrastructure is diverse and complex. It includes distributed networks, varied organizational structures and operating modes (including multinational ownership), interdependent functions and systems in both the physical space and cyberspace, and governance structures that involve multi-tier authorities, responsibilities, and regulations. Critical infrastructure owners and operators are uniquely positioned to manage risks to their individual operations and assets, and to determine effective strategies to make them more secure and resilient.
Critical infrastructure must be secure and able to withstand and rapidly recover from all hazards. Achieving this will require integration with the national preparedness system across prevention, protection, mitigation, response, and recovery.
This directive establishes national policy on critical infrastructure security and resilience. This embrace is a shared responsibility among the Federal, State, local, and territorial (S/L/T) entities, and private and public owners and operators of critical infrastructure. These entities are referred to as "critical infrastructure owners and operators." The directive identifies the critical infrastructure assets, functions, roles, and responsibilities across the Federal Government, as well as relevant state, territorial, and local governments. The Federal Government, and the States, have a responsibility to strengthen the security and resilience of its own critical infrastructure, for the continuity of national essential functions, and to integrate with its partner efforts and add value to the security and resilience efforts of critical infrastructure owners and operators.
Purpose
It is the policy of the United States to strengthen the security and resilience of its critical infrastructure against both physical and cyber threats. The Federal Government shall work with critical infrastructure owners and operators and S/L/T entities to take proactive steps to manage risk and strengthen the security and resilience of the nation's critical infrastructure, considering all hazards that could have a debilitating impact on national security, economic stability, public health and safety, or any combination thereof. These efforts shall seek to reduce vulnerabilities, minimize consequences, identify and design threats, and hasten response and recovery efforts related to critical infrastructure.

7

Esc

7



University of Colorado
Colorado Springs

CS4950/5950

Homeland Security & Cybersecurity

Drinking Water Infrastructure


- Except for its regulatory authorities under the previously cited laws, the **EPA has no authority to direct industry to implement specific security improvements or meet particular security standards.**
- As a general statement of policy, infrastructure owners and operators work with the EPA on a voluntary basis.



8

Esc

8




University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity


Drinking Water Infrastructure

A Water **Information Sharing and Analysis Center** with about 530 subscribing utilities help foster security cooperation and is the primary means for sharing information with the water sector.




WaterISAC

Water Security Network

9


9





University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity


Drinking Water Infrastructure

- In February 2013, President Obama signed Executive Order 13636 titled "Improving Critical Infrastructure Cybersecurity".
- EO 13636** directed the National Institute of Standards and Technology to develop a **Cybersecurity Framework** to form the basis of a Voluntary Critical Infrastructure Cybersecurity Program.



10


10

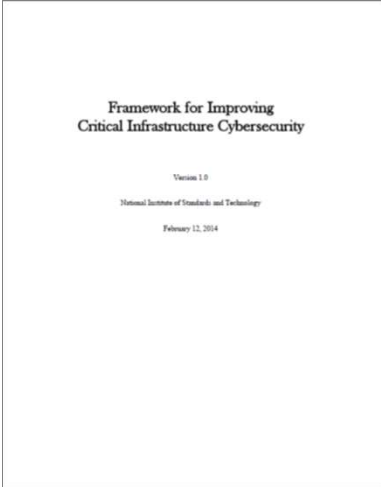


University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity


Drinking Water Infrastructure

- NIST released version 1.0 of the framework a year later in February 2014.
- The executive order also required Federal agencies with regulatory authority to **evaluate whether the NIST Cybersecurity Framework could and should be made mandatory** within their respective sectors.



11
Esc

11




University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Drinking Water Infrastructure

Of course the EPA did not have the authority but responded to the President's order that it would continue working with the water sector in a **voluntary manner** to manage cybersecurity risks.



12
Esc


12

UCCS University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Conclusion

Questions?



13

Esc