GANNETT FLEMING

Water & Wastewater Systems

Cross-Sector Interdependencies & Cyber Security Considerations

NJWEA John J. Lagrosa 107th Conference & Exposition
Atlantic City, New Jersey
June 9 – 10, 2022

Purpose and Learning Objectives

The purpose of this presentation is to:

- Discuss resilience within the Water/Wastewater Sector.
- Understand cross-sector interdependencies.
- Address prioritization of critical support services.
- Review one example of an industry approved cybersecurity framework.

At the end of this presentation, you will be able to:

- Identify cross-sector interdependencies to the Water/Wastewater Sector.
- Understand how to select an appropriate security framework.
- Understand the major components of a cybersecurity framework.

Chris Shepherd, PMP, CVI

35+ years experience

Operations project management; Regulatory compliance; Information/physical security

- Hazardous Liquid / Natural Gas Pipeline
- Water / Wastewater
- Electric Power Generation and Transmission
- Transit and Rail

AFFLIATIONS

North American Electric Reliability Corporation (NERC)

- Three terms on the Reliability Issues Steering Committee (RISC)
- Prior voting member on the Reliability and Security Technical Committee (RSTC)
- Co-author industry guidelines

American Public Transportation Association (APTA)

- Control and Communications Security Working Group (CCSWG)
- Enterprise Cyber Security Working Group (ECSWG)
- Co-author industry guidelines

Agenda

- Terminology
- Resilience - Water/Wastewater Sector
- Cross-sector interdependencies
- Cybersecurity considerations
- Prioritization of critical support services
- Review an industry approved cybersecurity framework

Terminology

Terminology

Resilience

The capacity to recover quickly from difficulties.

Toughness.

1) Advance the development of sector-specific cybersecurity resources

2) Raise awareness of the Water Sector as a lifeline sector and recognize the priority status of its needs and capabilities, and

3) Support the development and deployment of tools, training, and other assistance necessary to enhance preparedness and resilience.

Information Protection versus Cybersecurity

Information Protection

Protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to ensure confidentiality, integrity, and availability.

Cybersecurity

Prevention of damage to, protection of, and restoration of computers, electronic communications systems and services, wire communication, and electronic communication, including information contained therein, to ensure its confidentiality, availability, integrity, authentication, and nonrepudiation.

Confidentiality, Integrity, Availability

Confidentiality

Preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

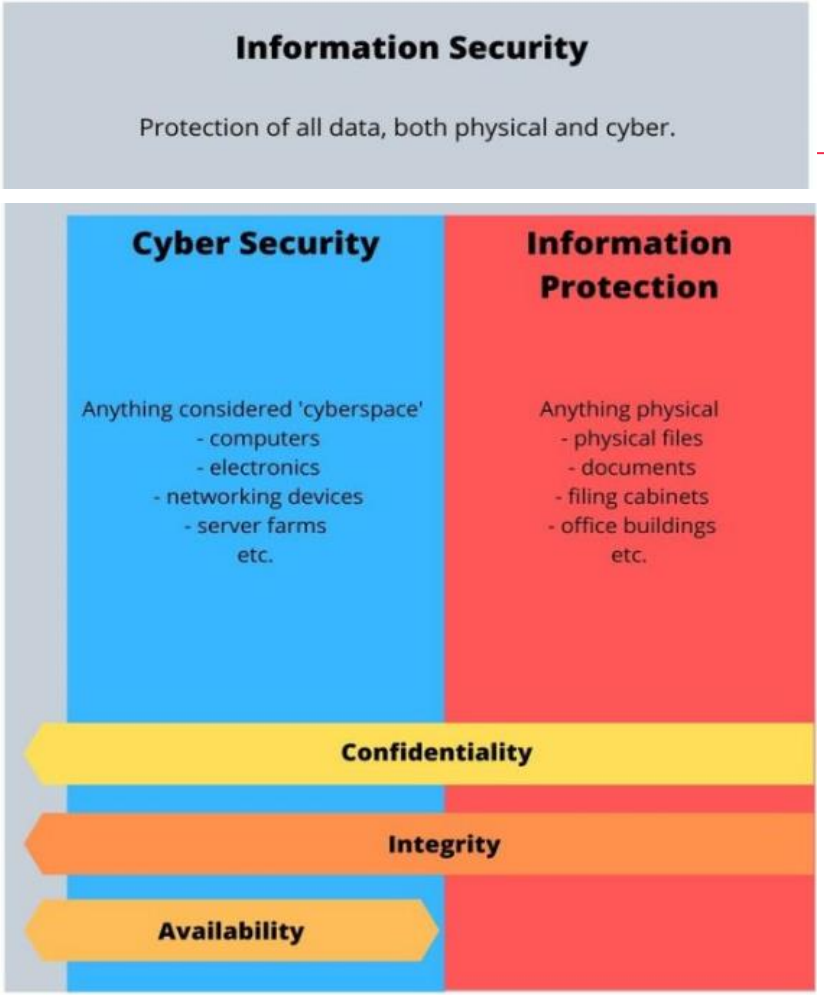
Integrity

Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity;

Availability

Ensuring timely and reliable access to and use of information.

Terminology



Credit to: https://infosecjon.com/information-security-vs-cyber-security/

Resilience - Water/Wastewater Sector

Resilience

The capacity to recover quickly from difficulties.

Toughness.

Resilience – National Critical Function (NCF)

Ensuring the supply of safe drinking water and treatment of wastewater is essential to modern life and the Nation's economy.

More than 150,000 public water systems provide drinking water to hundreds of millions of Americans.

U.S. wastewater treatment facilities process approximately 34 billion gallons of wastewater.

NCF to supply water and manage wastewater as vital to securing the population.

IBM X-Fore Threat Intelligence Index

Resilience

Cybersecurity programs are effective in eliminating vulnerabilities that cyber-attacks exploit.

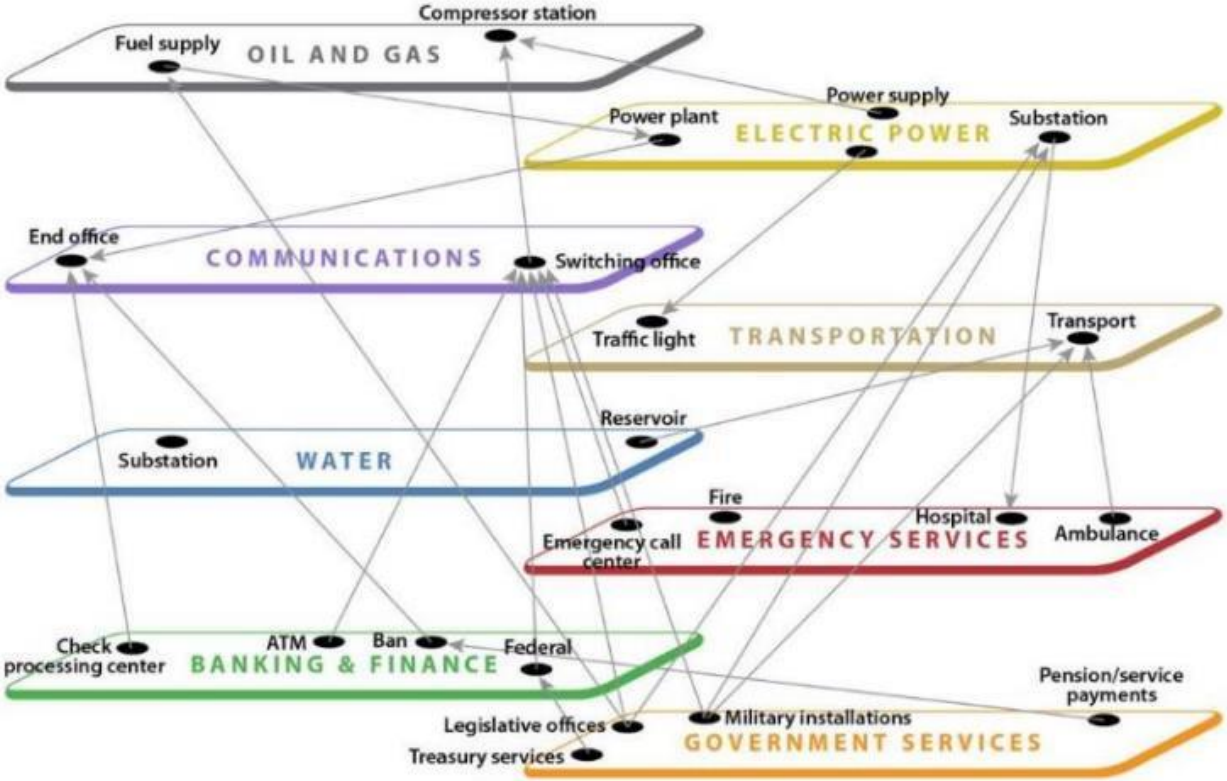
A basic cybersecurity program will:

- Ensure the integrity of process control systems
- Protect sensitive utility and customer information,
- Reduce legal liabilities if customer or employee personal information is stolen, and
- Maintain customer confidence.

IBM X-Fore Threat Intelligence Index

Cross-Sector Interdependencies

Understanding Sector Interdependencies

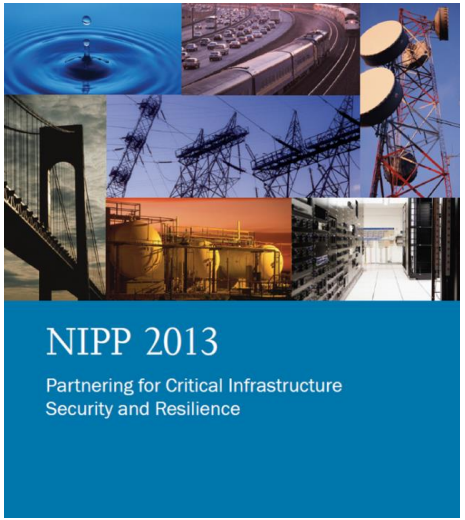


National Infrastructure Protection Plan (NIPP)

The National Infrastructure Protection Plan (NIPP) provides a unifying framework that integrates a range of efforts designed to enhance the safety of our nation's critical infrastructure.

There are 16 Sector Specific Plans

The Sector Specific Plans (SSPs) detail how the NIPP risk management framework is implemented within the context of the unique characteristics and risk landscape of each critical infrastructure sector.



The NIPP outlines how government and private sector participants in the critical infrastructure community work together to manage risks and achieve security and resilience outcomes.

 Chemical Sector	 Commercial Facilities Sector	 Communications Sector	 Critical Manufacturing Sector
 Dams Sector	 Defense Industrial Base Sector	 Emergency Services Sector	 Energy Sector
 Financial Services Sector	 Food and Agriculture Sector	 Government Facilities Sector	 Healthcare & Public Health
 Information Technology Sector	 Nuclear Reactors, Materials, Waste	 Transportation Systems Sector	 Water/Wastewater Systems

GANNETT FLEMING

Interdependencies

The Water and Wastewater Sector shares dependencies and interdependencies with each of the other 15 critical infrastructure sectors.

Primarily:

- Chemical
- Energy
- Food and Agriculture
- Healthcare and Public Health
- Transportation Systems
- Dams
- Information Technology
- Emergency Services sectors.

Terminology

Lifeline Critical Infrastructure Sectors

Reliable operations are so critical that a disruption or loss of one of these functions will directly affect the security and resilience of critical infrastructure within and across numerous sectors.

There are four designated lifeline functions

- **Transportation**
- **Water**
- **Energy**
- **Communications**

 Chemical Sector	 Commercial Facilities Sector	 Communications Sector	 Critical Manufacturing Sector
 Dams Sector	 Defense Industrial Base Sector	 Emergency Services Sector	 Energy Sector
 Financial Services Sector	 Food and Agriculture Sector	 Government Facilities Sector	 Healthcare & Public Health
 Information Technology Sector	 Nuclear Reactors, Materials, Waste	 Transportation Systems Sector	 Water/Wastewater Systems

GANNETT FLEMING

Cybersecurity Considerations

Water / Wastewater Systems Sector

The Water / Wastewater Systems Sector is vulnerable to a variety of direct attacks, including:

- Contamination with deadly agents
- Physical attacks, such as the release of toxic gaseous chemicals
- Natural disasters
- Cyberattacks

Water / Wastewater Systems Sector

Water management is prone to indirect operational impacts due to attacks on interdependent CISA Sectors/industries.

Water/Wastewater impacts other Critical Infrastructure sectors

- Energy
- Food & Agriculture
- Transportation

Aurora Cyber Vulnerability

https://www.youtube.com/watch?v=bAWU5aMyAAo

March 4, 2007 - Idaho National Laboratory ran the Aurora Generator Test to demonstrate how a cyber attack could destroy physical components of the electric grid.

The experiment used a computer program to rapidly open and close a 2.25 MW diesel generator's circuit breakers out of phase from the rest of the grid and cause it to fail.

This vulnerability is referred to as the Aurora Vulnerability and is caused through bypassing protective relays.

GANNETT FLEMING

Cyber Threats to the Water / Wastewater Infrastructure

Top Five Threats

- Ransomware
- Phishing
- Data Leakage
- Hacking
- Insider Threat

Prioritization of Critical Support Services

Reliability

What is the reliability of water/wastewater?

The reliability of water/wastewater supply systems is considered in two aspects:

- System adequacy
- System security

Water/Wastewater systems contain many components that are divided into:

- **Physical**
- **Cyber, and**
- **Human elements.**

This includes **supply chain vendor management.**

GANNETT FLEMING

Reliability

Note that resilience to disasters, service interruptions, or other adverse events are often incorporated into these elements to ensure reliable and sustainable supplies and services to customers.

Physical Elements

- Water source
- Conveyance
- Raw water storage
- Treatment
- Finished water storage
- Distribution systems
- Monitoring systems

Reliability

Cyber Elements

- Supervisory Control and Data Acquisition (SCADA) Systems
- Process systems and operational controls
- Enterprise systems

Human Elements

- Employees and contractors
  - Availability
  - Skillsets
  - Subject matter experts
  - Laboratory analysis

GANNETT FLEMING

Reliability

Supply Chain and Vendor Management

- Water source
- Energy - Electricity, Natural gas
- Chemicals
- Testing
- Managed Services
- Contract Management
- Transportation
- Commercial Facilities
- Communications
- Manufacturing
- Emergency Services

GANNETT FLEMING

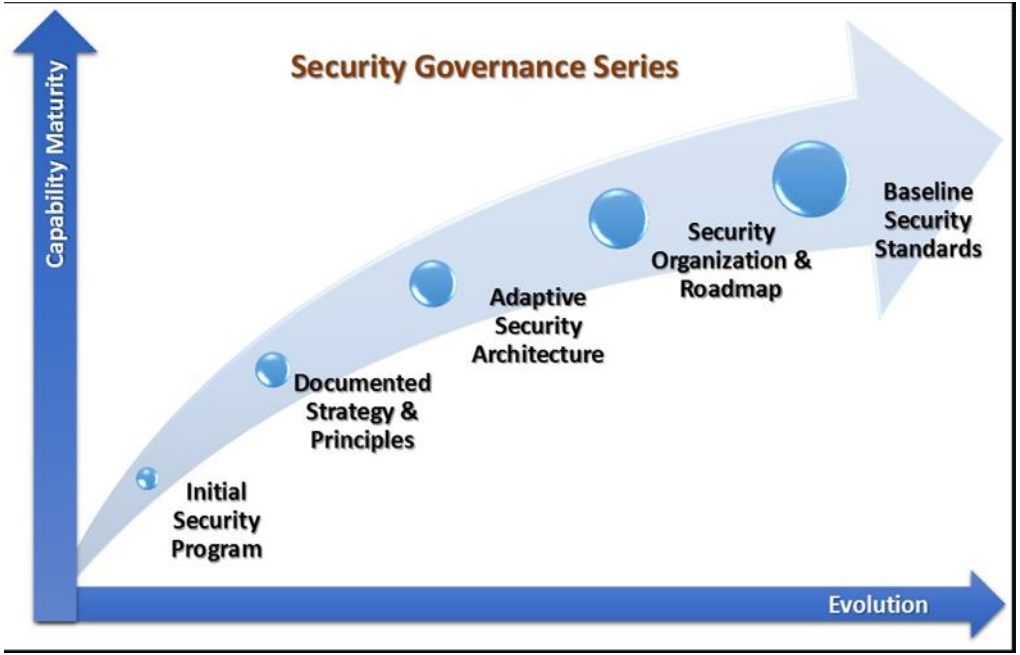
Review an Industry Approved Cybersecurity Framework

Controls for Critical Infrastructure

GANNETT FLEMING

Cybersecurity Maturity Model

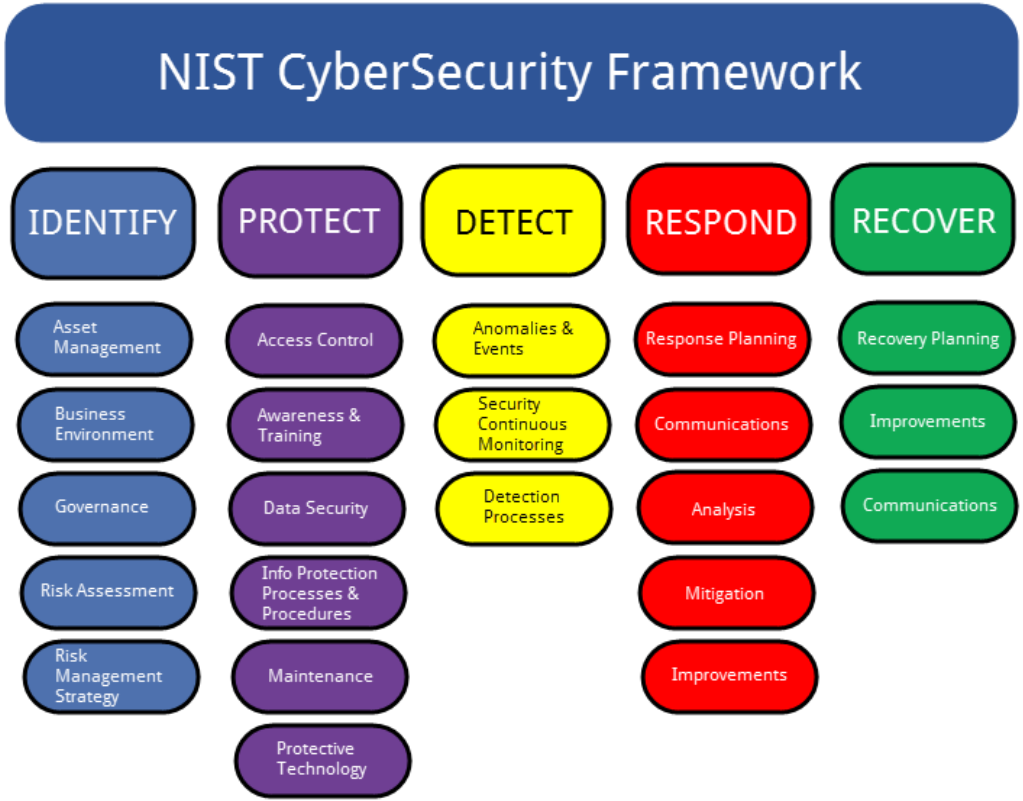
Provides a method for reporting incremental improvement in cybersecurity protections and enables organization to periodically assess maturity status.



One Example - NIST Cybersecurity Framework

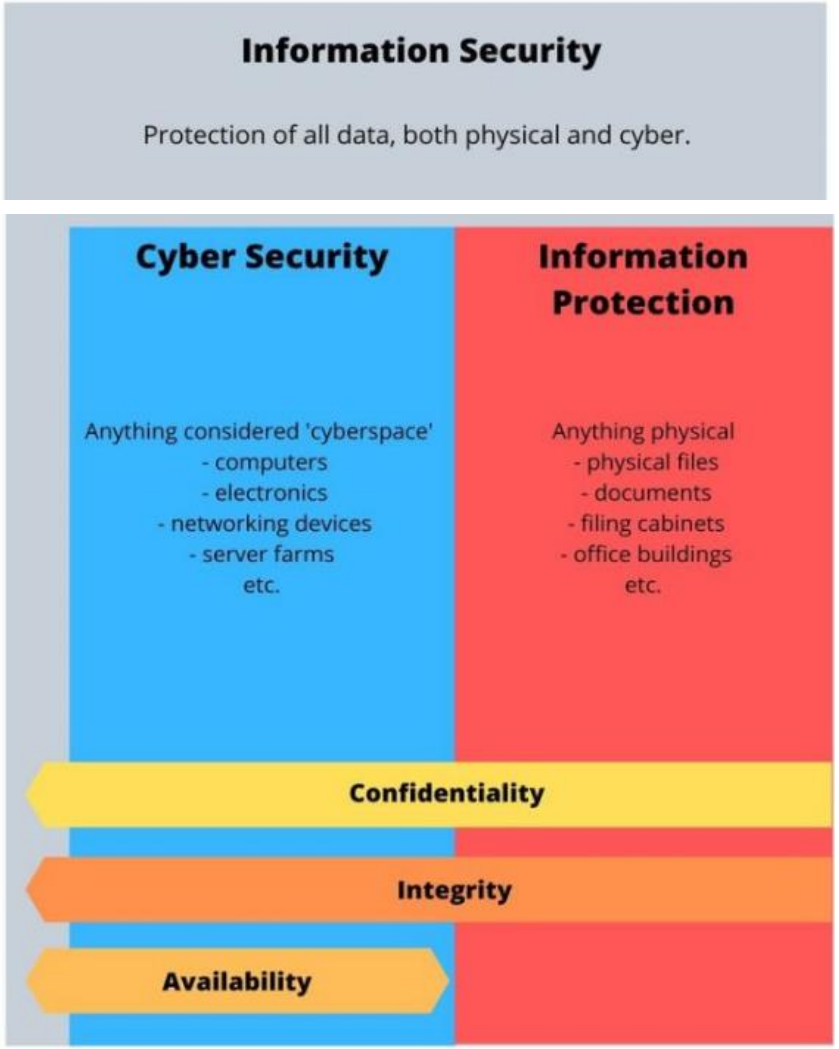
Five (5) Control Functions

23 Categories



Cybersecurity Framework – Benefits

- Recognized framework used for voluntary adoption of security controls
- Leverages existing cyber and physical control environment
- Can be tailored to current operations based on risk-based decisions
- Scalable for future adoption of other cybersecurity frameworks, if required
- SCADA-specific security controls can be incorporated



Summary and Review

The purpose of this presentation was to:

- Discuss resilience within the Water/Wastewater Sector.
- Understand cross-sector interdependencies.
- Address prioritization of critical support services.
- Review one example of an industry approved cybersecurity framework.

You should now be able to:

- Identify cross-sector interdependencies to the Water/Wastewater Sector.
- Understand how to select an appropriate security framework.
- Understand the major components of a cybersecurity framework.

Primary Reference Materials

- EPA Cybersecurity Best Practices for Water Sector
- American Water Infrastructure Act of 2018 Requirements
- NIST Cybersecurity Framework (CSF)
- DHS – CISA Sectors
- Water/Wastewater Sector
- Water ISAC – Water Security
- NIAC – Water Sector Resilience

GANNETT FLEMING

Water & Wastewater Systems

Cyber Security Considerations

Chris Shepherd, PMP, CVI
Sr. Information Security Manager
Cybersecurity Compliance

LShepherd@gfnet.com
503.207.3862