Cyber Security in 2022

Presented by

Britton Electronics & Automation Inc.

What is Cyber Security?

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.

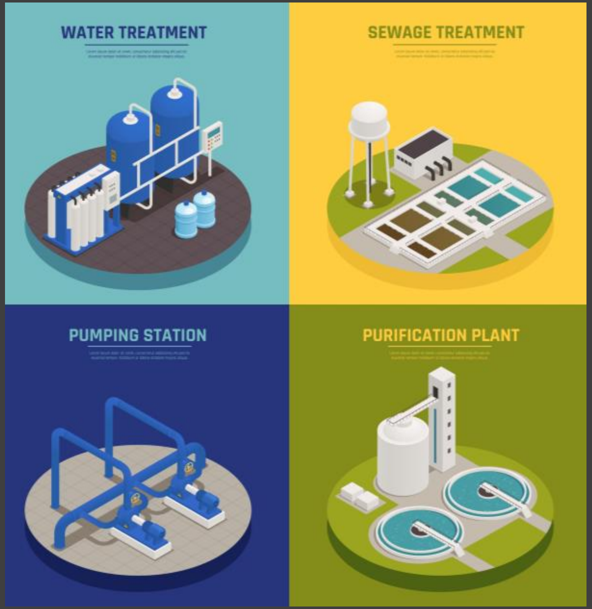
Implementing effective cybersecurity measures is particularly challenging today because there are more devices than people, and attackers are becoming more innovative.

Overview:

Within the last several decades, cybersecurity threats, including such things as cyber-terrorism and ransomware attacks, have grown from the esoteric practice of a few specialists to a problem of general concern. Critical infrastructure systems serving the people of the United States have been found to be particularly vulnerable to such attacks.

"Government intelligence confirms the water and wastewater sector is under a direct threat as part of a foreign government's multi-stage intrusion campaign, and individual criminal actors and groups threaten the security of our nation's water and wastewater systems' operations and data."

In response to the general threat to critical infrastructure, a wide array of standards and guidelines are available to assist organizations with implementing security controls to mitigate the risk from cyber-attacks.



Cybersecurity Myths

The volume of cybersecurity incidents is on the rise across the globe, but misconceptions continue to persist, including the notion that:

Cybercriminals are outsiders

Cybersecurity breaches are often the result of malicious insiders, working for themselves or in concert with outside hackers. These insiders can be a part of well-organized groups, backed by nation-states.

Cybersecurity Myths

Risks are well-known
In fact, the risk surface is still expanding, with thousands of new vulnerabilities being reported in old and new applications and devices. And opportunities for human error - specifically by negligent employees or contractors who unintentionally cause a data breach - keep increasing.

Attack vectors are contained
Cybercriminals are finding new attack vectors all the time - including Linux systems, operational technology (OT), Internet of Things (IoT) devices, and cloud environments.

My industry is safe
Every industry has its share of cybersecurity risks, with cyber adversaries exploiting the necessities of communication networks within almost every government and private-sector organization. For example, ransomware attacks (see below) are targeting more sectors than ever, including local governments and non-profits, and threats on supply chains, ".gov" websites, and critical infrastructure have also increased.

Common Cyber Threats

Although cybersecurity professionals work hard to close security gaps, attackers are always looking for new ways to escape IT notice, evade defense measures, and exploit emerging weaknesses. The latest cybersecurity threats are putting a new spin on "known" threats, taking advantage of work-from-home environments, remote access tools, and new cloud services. These evolving threats include:

Malware

The term "malware" refers to malicious software variants—such as worms, viruses, Trojans, and spyware—that provide unauthorized access or cause damage to a computer. Malware attacks are increasingly "fileless" and designed to get around familiar detection methods, such as antivirus tools, that scan for malicious file attachments.

Ransomware

Ransomware is a type of malware that locks down files, data or systems, and threatens to erase or destroy the data - or make private or sensitive data to the public - unless a ransom is paid to the cybercriminals who launched the attack. Recent ransomware attacks have targeted state and local governments, which are easier to breach than organizations and under pressure to pay ransoms in order to restore applications and web sites on which citizens rely.

Common Cyber Threats

Phishing / social engineering

Phishing is a form of social engineering that tricks users into providing their own PII or sensitive information. In phishing scams, emails or text messages appear to be from a legitimate company asking for sensitive information, such as credit card data or login information. The FBI has noted about a surge in pandemic-related phishing, tied to the growth of remote work.

Insider threats

Current or former employees, business partners, contractors, or anyone who has had access to systems or networks in the past can be considered an insider threat if they abuse their access permissions. Insider threats can be invisible to traditional security solutions like firewalls and intrusion detection systems, which focus on external threats.

Common Cyber Threats

Distributed denial-of-service (DDoS) attacks

A DDoS attack attempts to crash a server, website or network by overloading it with traffic, usually from multiple coordinated systems. DDoS attacks overwhelm enterprise networks via the simple network management protocol (SNMP), used for modems, printers, switches, routers, and servers.

Advanced persistent threats (APTs)

In an APT, an intruder or group of intruders infiltrate a system and remain undetected for an extended period. The intruder leaves networks and systems intact so that the intruder can spy on business activity and steal sensitive data while avoiding the activation of defensive countermeasures. The recent Solar Winds breach of United States government systems is an example of an APT.

Man-in-the-middle attacks

Man-in-the-middle is an eavesdropping attack, where a cybercriminal intercepts and relays messages between two parties in order to steal data. For example, on an unsecure Wi-Fi network, an attacker can intercept data being passed between guest's device and the network.

Hacker Tries to Poison California Water System

On Jan. 15, 2021, a hacker tried to poison a water treatment plant that served parts of the San Francisco Bay Area. It didn't seem hard.

The hacker had the username and password for a former employee's TeamViewer account, a popular program that lets users remotely control their computers, according to a private report compiled by the Northern California Regional Intelligence Center in February

After logging in, the hacker, whose name and motive are unknown and who hasn't been identified by law enforcement, deleted programs that the water plant used to treat drinking water.

Florida Hack Exposes Danger to Water Systems

A renegade mouse cursor signaled the danger at the water treatment plant in Oldsmar, Florida.

On Feb. 5, 2021, a plant operator for the city of about 15,000 on Florida’s west coast saw his cursor being moved around on his computer screen, opening various software functions that control the water being treated. The intruder boosted the level of sodium hydroxide—or lye—in the water supply to 100 times higher than normal.

Sodium hydroxide, the main ingredient in liquid drain cleaners, is used to control water acidity and remove metals from drinking water in treatment plants. Lye poisoning can cause burns, vomiting, severe pain and bleeding.

After the hacker exited the computer, the operator immediately reduced the sodium hydroxide back to its normal level and then notified his supervisor, Pinellas County Sheriff Bob Gualtieri said at a news conference a few days later. Even if it hadn’t been quickly reversed, the system has safeguards and the water would have been checked before it was released, so the public was never at risk, he added.

How Did They Do it?

- Unsecured credentials.
  - Ex-Employ credentials were not disabled
  - Credentials were shared
- Lack of policies and procedures for remote access to system

Recommendations

Telecommunications, Network Security, and Architecture

- This category is concerned with the security of the network infrastructure from the data connector on the wall to the enterprise switches, routers, and firewalls. This includes the physical security of the cables, the telecom closets, and the computer rooms, and the protection of the data as it travels on public channels and wireless circuits. Spam filtering and website blocking are also included in this category.
- The focus of this category is establishing a “defense-in-depth” network architecture with the network at its core. It also addresses adherence to new standards for PCS network security, particularly network topology requirements within the vicinity of PCS systems and PLC controls. Another area addressed in this category is network management, including port level security.

Education

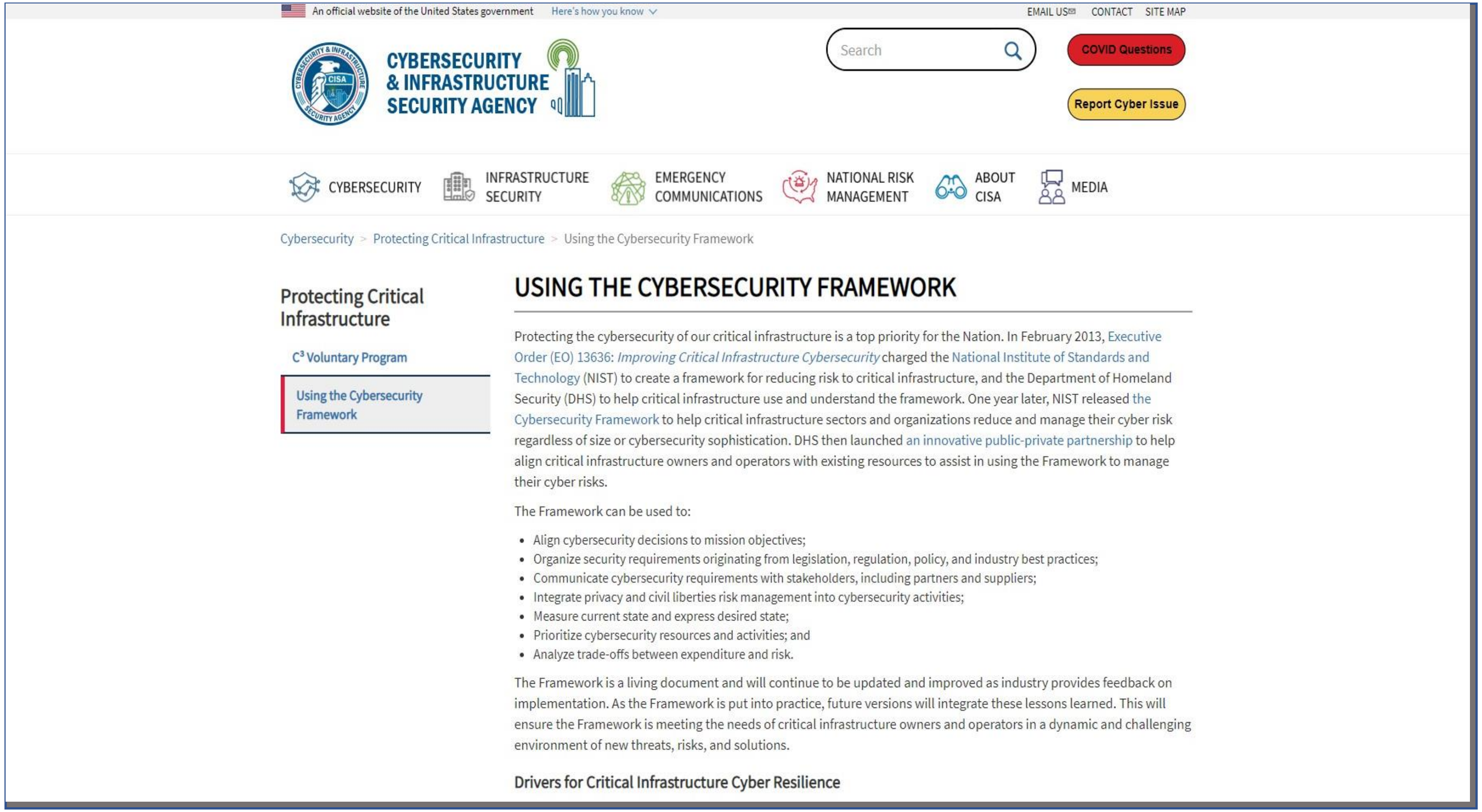
- This category is concerned with bringing security awareness to the employees, clients, and service providers of the organization.
- Education involves identifying best practices and providing formal training on the security policies and procedures of the enterprise as well as security awareness and incident response. It involves test practice of the key security processes and actions to ensure quick and accurate response to security incidents within the enterprise.

Managing Cyber Risks & Boosting Resilience

Protecting critical infrastructure

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

Managing Cyber Risks & Boosting Resilience


An official website of the United States government
Here's how you know
EMAIL US
CONTACT
SITE MAP
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
Search
COVID Questions
Report Cyber Issue
CYBERSECURITY
INFRASTRUCTURE SECURITY
EMERGENCY COMMUNICATIONS
NATIONAL RISK MANAGEMENT
ABOUT CISA
MEDIA
Cybersecurity > Protecting Critical Infrastructure > Using the Cybersecurity Framework
Protecting Critical Infrastructure
C³ Voluntary Program
Using the Cybersecurity Framework

USING THE CYBERSECURITY FRAMEWORK

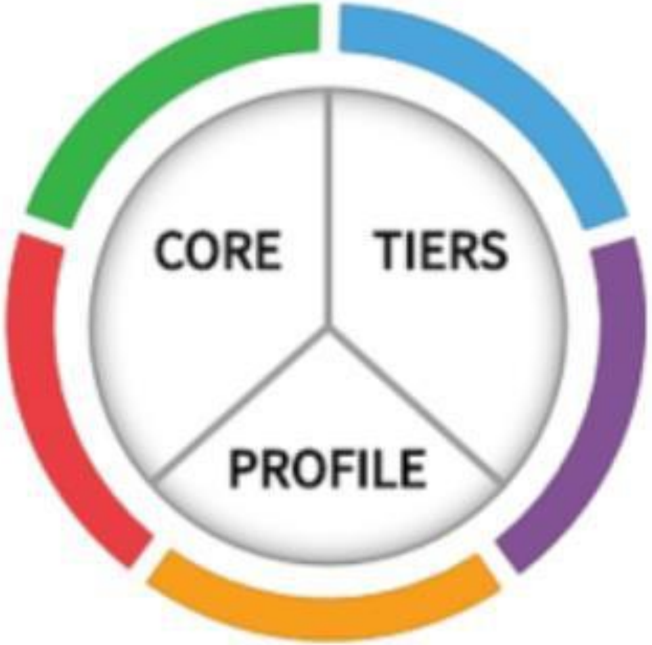
Protecting the cybersecurity of our critical infrastructure is a top priority for the Nation. In February 2013, Executive Order (EO) 13636: *Improving Critical Infrastructure Cybersecurity* charged the National Institute of Standards and Technology (NIST) to create a framework for reducing risk to critical infrastructure, and the Department of Homeland Security (DHS) to help critical infrastructure use and understand the framework. One year later, NIST released the Cybersecurity Framework to help critical infrastructure sectors and organizations reduce and manage their cyber risk regardless of size or cybersecurity sophistication. DHS then launched an innovative public-private partnership to help align critical infrastructure owners and operators with existing resources to assist in using the Framework to manage their cyber risks.

The Framework can be used to:

- Align cybersecurity decisions to mission objectives;
- Organize security requirements originating from legislation, regulation, policy, and industry best practices;
- Communicate cybersecurity requirements with stakeholders, including partners and suppliers;
- Integrate privacy and civil liberties risk management into cybersecurity activities;
- Measure current state and express desired state;
- Prioritize cybersecurity resources and activities; and
- Analyze trade-offs between expenditure and risk.

The Framework is a living document and will continue to be updated and improved as industry provides feedback on implementation. As the Framework is put into practice, future versions will integrate these lessons learned. This will ensure the Framework is meeting the needs of critical infrastructure owners and operators in a dynamic and challenging environment of new threats, risks, and solutions.

Drivers for Critical Infrastructure Cyber Resilience



Managing Cyber Risks & Boosting Resilience

Framework for Improving Critical Infrastructure Cybersecurity

- Voluntary, risk-based approach for managing cybersecurity risks for critical infrastructure
- References industry standards and best practices to help organizations manage cybersecurity risks
- Addresses broad security needs of all critical sectors but **is not a one-size-fits-all approach**. Sector-specific guidance needed to address unique needs of each sector
- More info: www.nist.gov/cyberframework

Managing Cyber Risks & Boosting Resilience

Resilience

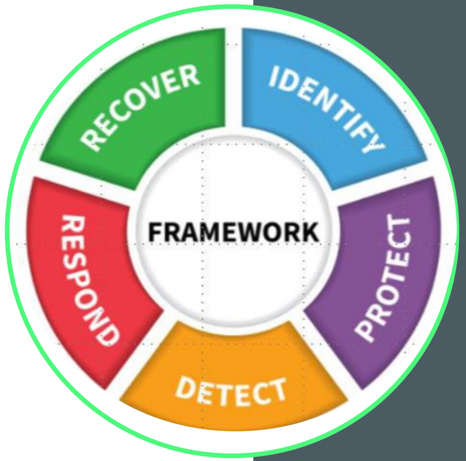
noun

1. the power or ability of a material to return to its original form, position, etc., after being bent, compressed, or stretched; elasticity.
2. the ability of a person to adjust to or recover readily from illness, adversity, major life changes, etc.; buoyancy.
3. **the ability of a system or organization to respond to or recover readily from a crisis, disruptive process, etc.**

Managing Cyber Risks & Boosting Resilience

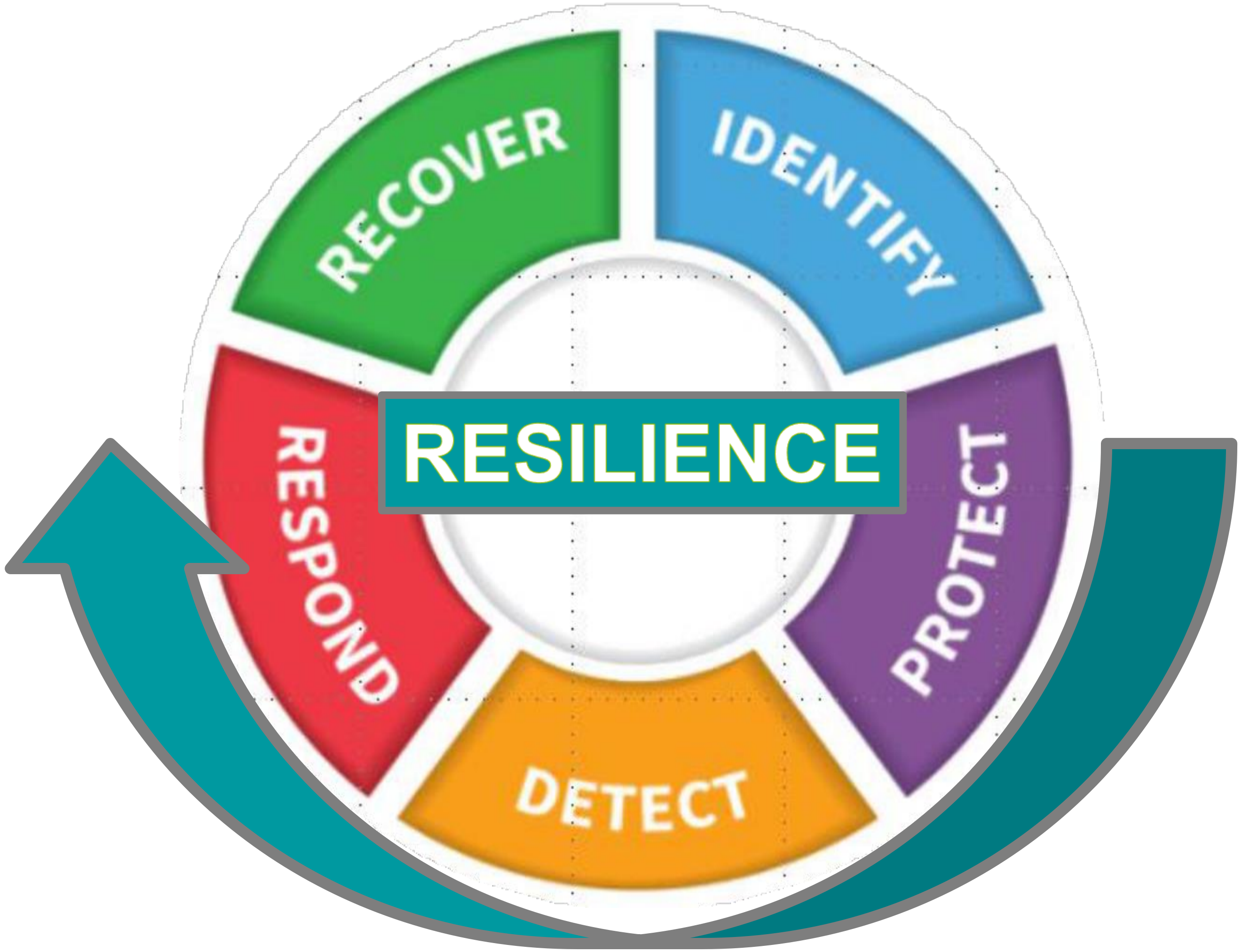
NIST Cybersecurity Framework Core

- Describes desired outcomes
- Understandable by everyone
- Applies to any type of risk management
- Defines the entire breadth of cybersecurity
- Spans both prevention and reaction



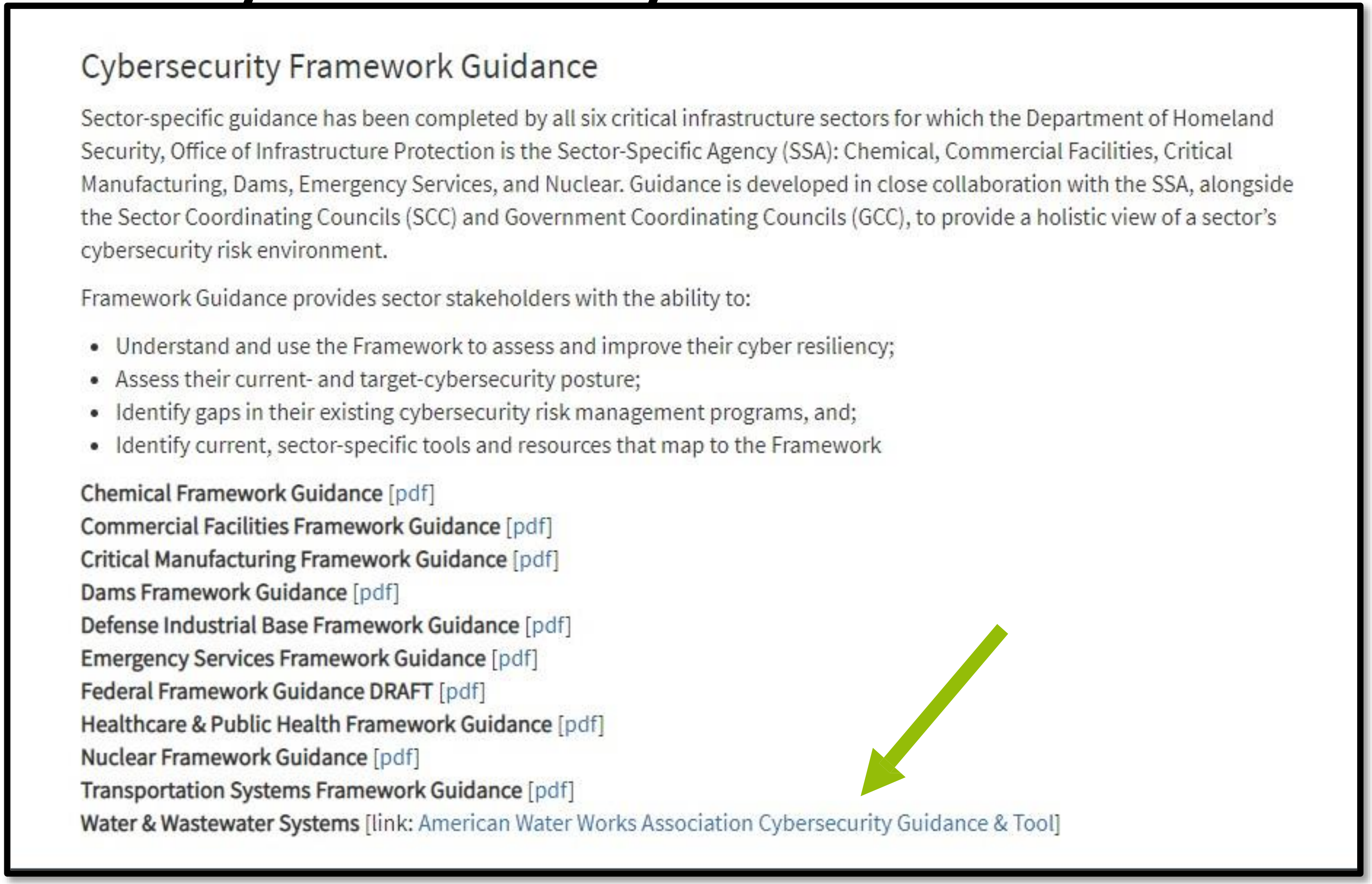
Managing Cyber Risks & Boosting Resilience

NIST Cybersecurity Framework Core



Managing Cyber Risks & Boosting Resilience

NIST Cybersecurity Framework Core



Cybersecurity Framework Guidance

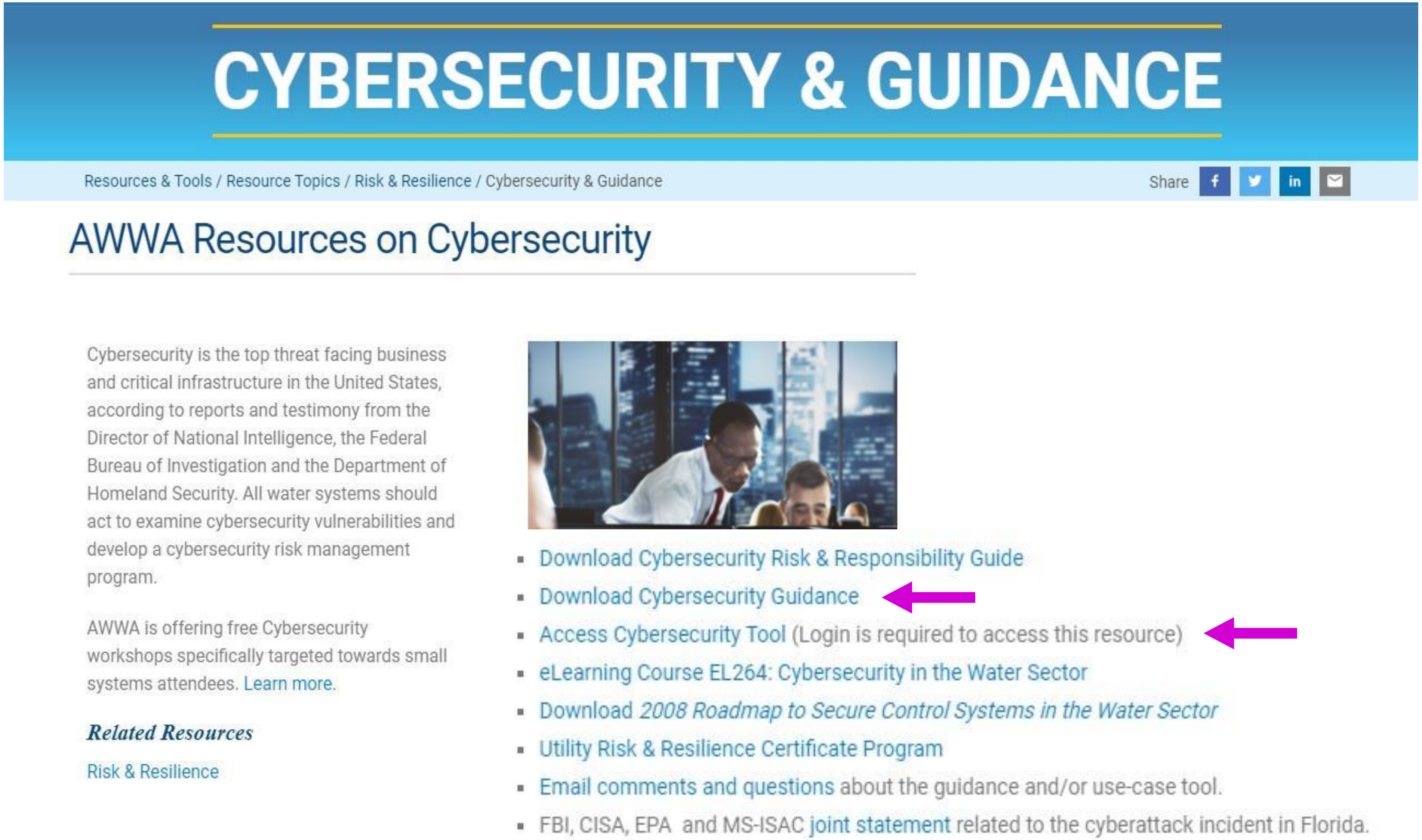
Sector-specific guidance has been completed by all six critical infrastructure sectors for which the Department of Homeland Security, Office of Infrastructure Protection is the Sector-Specific Agency (SSA): Chemical, Commercial Facilities, Critical Manufacturing, Dams, Emergency Services, and Nuclear. Guidance is developed in close collaboration with the SSA, alongside the Sector Coordinating Councils (SCC) and Government Coordinating Councils (GCC), to provide a holistic view of a sector's cybersecurity risk environment.

Framework Guidance provides sector stakeholders with the ability to:

- Understand and use the Framework to assess and improve their cyber resiliency;
- Assess their current- and target-cybersecurity posture;
- Identify gaps in their existing cybersecurity risk management programs, and;
- Identify current, sector-specific tools and resources that map to the Framework

Chemical Framework Guidance [pdf]
Commercial Facilities Framework Guidance [pdf]
Critical Manufacturing Framework Guidance [pdf]
Dams Framework Guidance [pdf]
Defense Industrial Base Framework Guidance [pdf]
Emergency Services Framework Guidance [pdf]
Federal Framework Guidance DRAFT [pdf]
Healthcare & Public Health Framework Guidance [pdf]
Nuclear Framework Guidance [pdf]
Transportation Systems Framework Guidance [pdf]
Water & Wastewater Systems [link: American Water Works Association Cybersecurity Guidance & Tool]

AWWA Cybersecurity Guidance



CYBERSECURITY & GUIDANCE

Resources & Tools / Resource Topics / Risk & Resilience / Cybersecurity & Guidance

AWWA Resources on Cybersecurity

Cybersecurity is the top threat facing business and critical infrastructure in the United States, according to reports and testimony from the Director of National Intelligence, the Federal Bureau of Investigation and the Department of Homeland Security. All water systems should act to examine cybersecurity vulnerabilities and develop a cybersecurity risk management program.

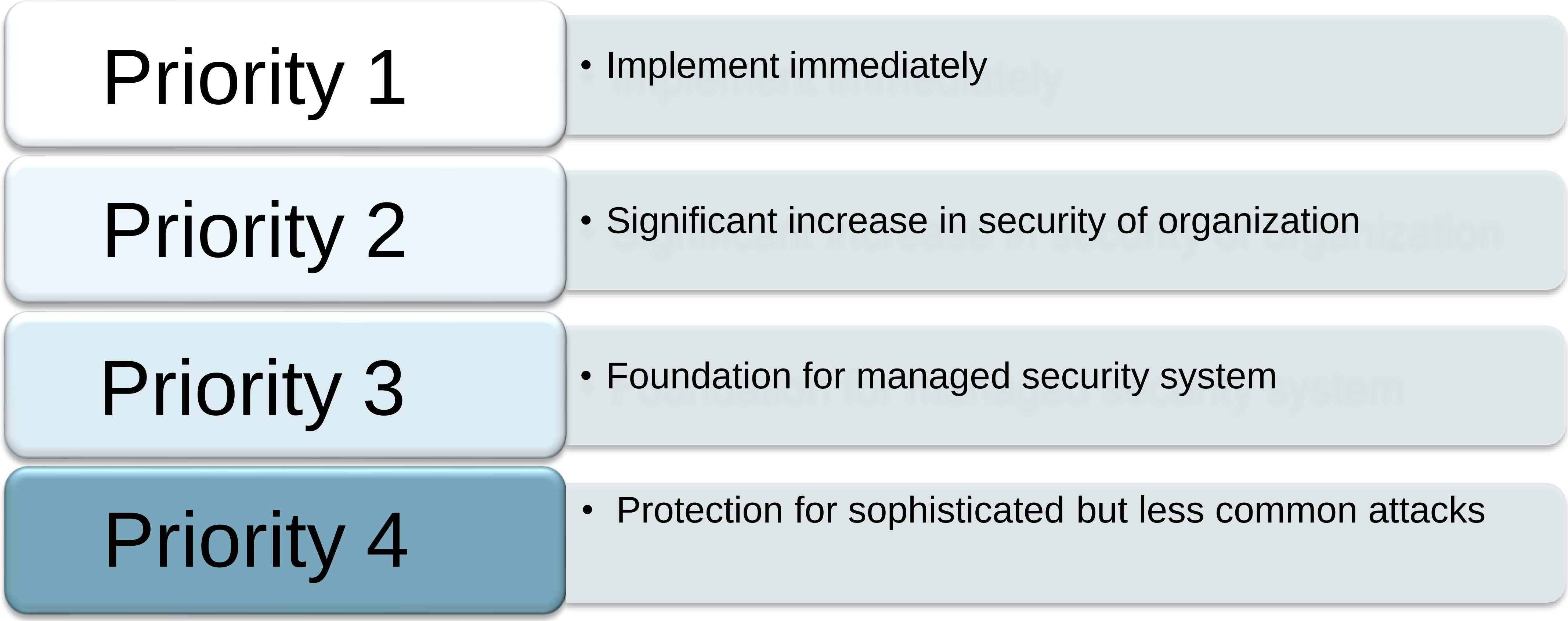
AWWA is offering free Cybersecurity workshops specifically targeted towards small systems attendees. Learn more.

Related Resources

Risk & Resilience

- Download Cybersecurity Risk & Responsibility Guide
- Download Cybersecurity Guidance
- Access Cybersecurity Tool (Login is required to access this resource)
- eLearning Course EL264: Cybersecurity in the Water Sector
- Download *2008 Roadmap to Secure Control Systems in the Water Sector*
- Utility Risk & Resilience Certificate Program
- Email comments and questions about the guidance and/or use-case tool.
- FBI, CISA, EPA and MS-ISAC joint statement related to the cyberattack incident in Florida.

Online Tool Output: Recommended priorities



Priority 1	• Implement immediately
Priority 2	• Significant increase in security of organization
Priority 3	• Foundation for managed security system
Priority 4	• Protection for sophisticated but less common attacks

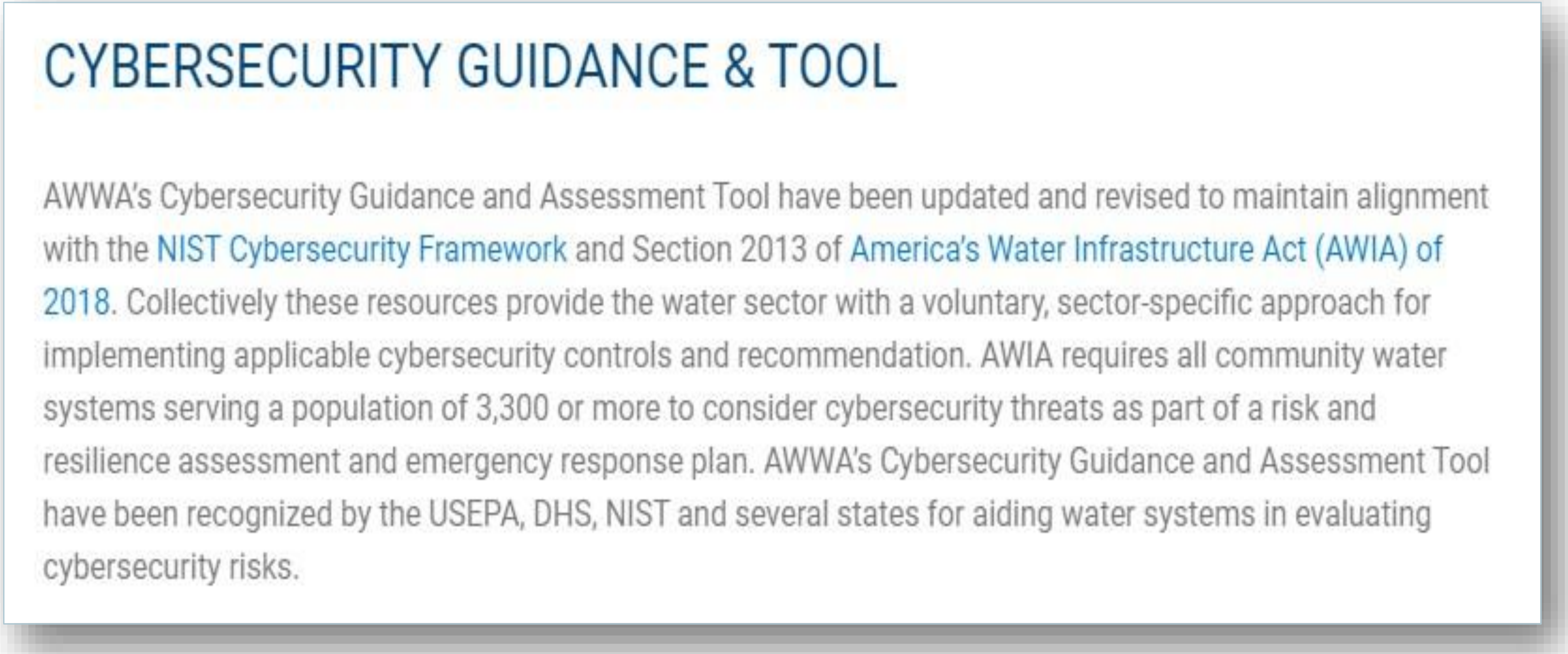
America’s Water Infrastructure Act (AWIA) 2018

§ 2013 Community Water System Risk And Resilience

Requires CWSs serving population > 3,300 to…

- Conduct & certify Risk & Resilience Assessment (RRA)
- Complete/revise & certify Emergency Response Plan (ERP)
- Must review, update & recertify every 5 years

AWWA Cybersecurity Guidance



CYBERSECURITY GUIDANCE & TOOL

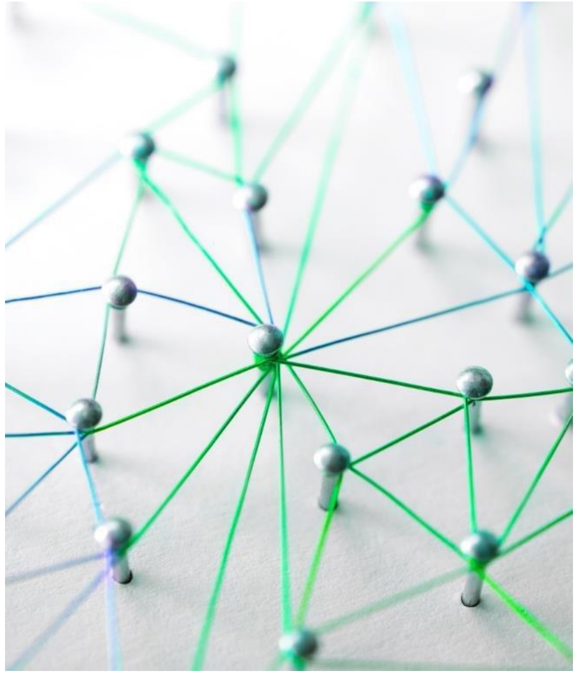
AWWA's Cybersecurity Guidance and Assessment Tool have been updated and revised to maintain alignment with the NIST Cybersecurity Framework and Section 2013 of America's Water Infrastructure Act (AWIA) of 2018. Collectively these resources provide the water sector with a voluntary, sector-specific approach for implementing applicable cybersecurity controls and recommendation. AWIA requires all community water systems serving a population of 3,300 or more to consider cybersecurity threats as part of a risk and resilience assessment and emergency response plan. AWWA's Cybersecurity Guidance and Assessment Tool have been recognized by the USEPA, DHS, NIST and several states for aiding water systems in evaluating cybersecurity risks.

CISA – Industrial Control Systems

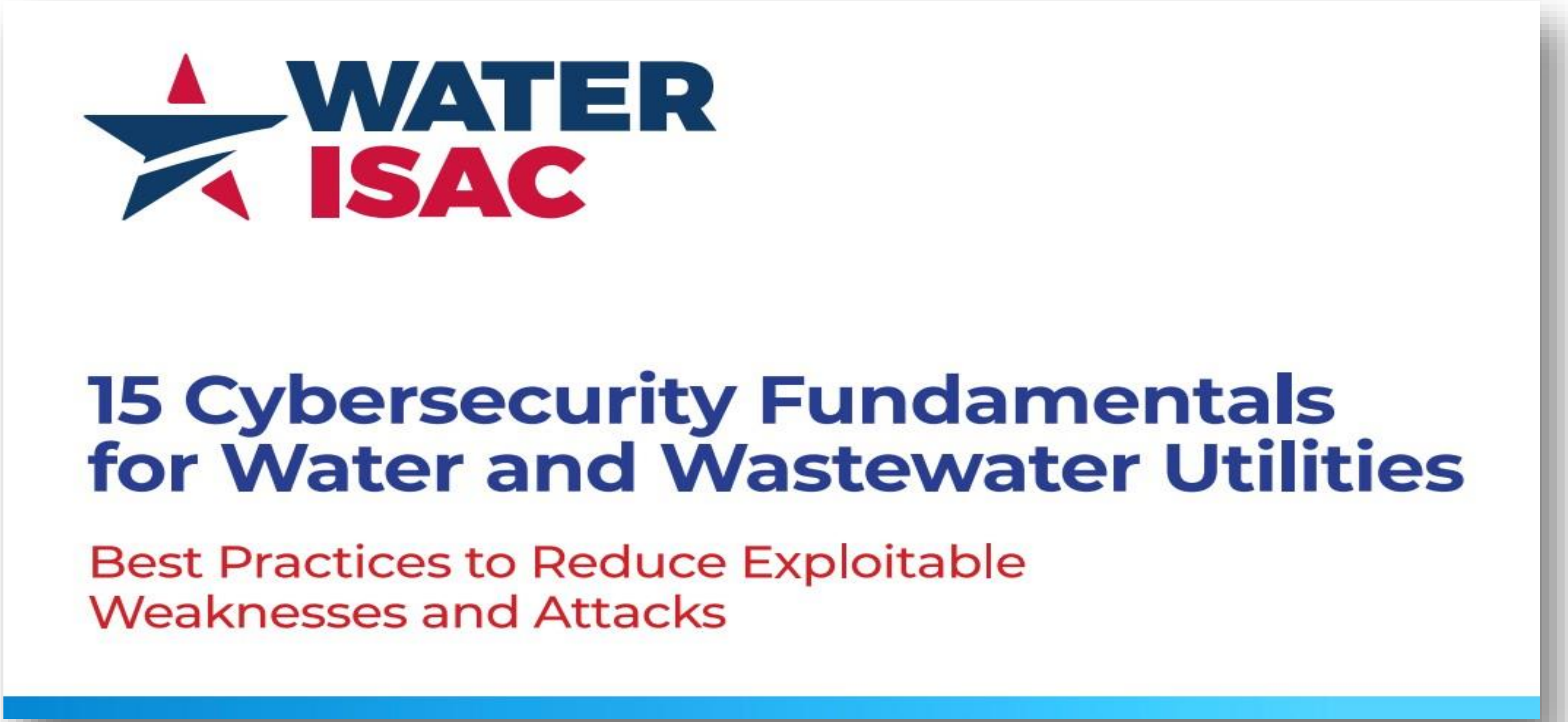
AWWA Online Tool / NIST CSF 1.1 / AWIA / CSET

AWWA Online Tool updates

- Updated in 2019
  - To incorporate changes to NIST CSF
  - 1.0 > 1.1
  - To aid in compliance with AWIA 2018
- October 2020 Integration of output into CSET



Many other resources available…



WATER ISAC

15 Cybersecurity Fundamentals for Water and Wastewater Utilities

Best Practices to Reduce Exploitable Weaknesses and Attacks

Summary

- Security is a process not a task! It is a journey not a destination!
- Security is not an absolute! It is a matter of degree.
- Neither practical nor feasible to fully mitigate all risks. Must allocate available resources as efficiently as possible.
- **Goal: Risk management and increased resilience for critical infrastructure.**

Question and Answer

Ask any question.

Thank You

Nick Towell
Phoenix Contacts

Automation Sales Engineer
ntowell@phoenixcontact.com

Robert Britton
Britton Electronics & Automation Inc.

Field Engineer
Robert@go-bea.com