American Water Works Association

Dedicated to the World's Most Important Resource®

Managing Cybersecurity Risks in the Water Sector

Learning Objectives

Recognize	Why cybersecurity is an important element of drinking water and wastewater utility operations and management
Explain	How AWWA's Guidance and Tool supports cybersecurity risk management
Identify	Cybersecurity resources, including support for small systems
Utilize	Recommended guidance to support implementation of a cybersecurity risk management plan

A. Cyber Threat Landscape

#1 Threat Facing Critical Infrastructure

- Intelligence threat assessment
  - Criminal: Financial Motivation
  - Malevolent: Operational Impact

- All is not lost, it about Risk Management not Risk Elimination
  - Best practices exist and need to be implemented

  - 100% Threat Likelihood…assume it will happen

Cyber Threat Landscape Snapshot

March 2021, Kansas Man Indicted for Tampering with Public Water System

- Terminated employee with active remote access credentials shut down the disinfection treatment process Post Rock Rural Water District.
- Hacker has been charged with one count of tampering with a public water system and one count of reckless damage to a protected computer during unauthorized access.

March 2021, Microsoft Exchange Exploit

- Four zero-day vulnerabilities in Microsoft Exchange Server were actively exploited by a state-sponsored threat group from China and appear to have been adopted by other cyberattackers in widespread attacks. Microsoft stated that the stolen credentials can allow attacker to hijack the system and execute commands remotely.

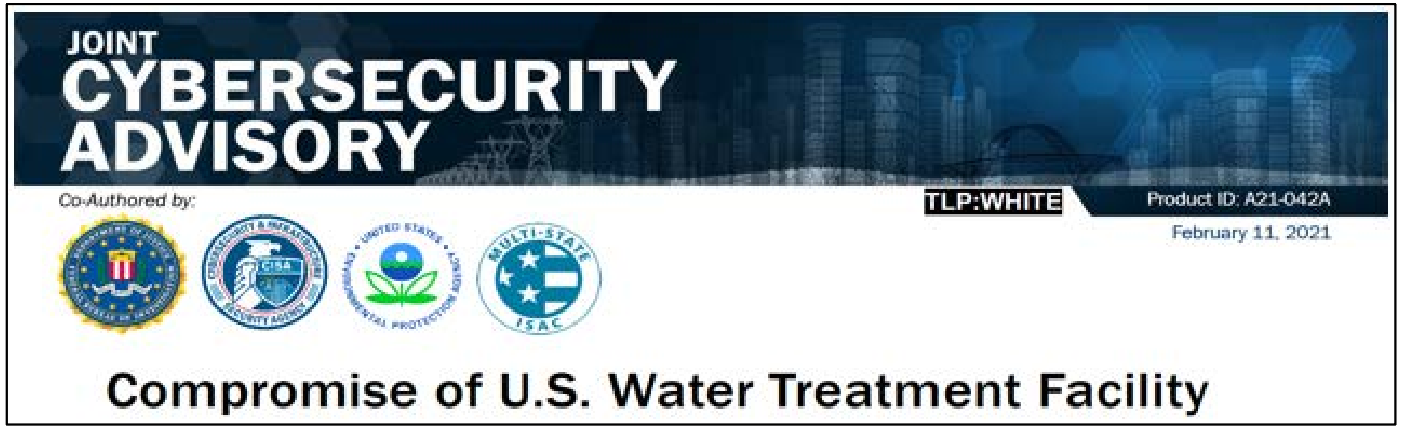
Feb 2021, Oldsmar (FL) Water Utility Operating System Breached

- Attempt to alter dosing of sodium hydroxide.
- Proximity to Superbowl brings major federal support and media attention

Dec 2020, Solarwinds Hack

- Russian attack compromises 18,000 entities including multiple Federal Agencies
- Highly sophisticated attack targeting the code in update for IT software mgt system

OLDSMAR, FLORIDA CYBER INCIDENT – FEB 5, 2021



JOINT
CYBERSECURITY
ADVISORY

Co-Authored by:

TLP:WHITE

Product ID: A21-042A

February 11, 2021

Compromise of U.S. Water Treatment Facility

What happened?

- Unauthorized access to SCADA by unknown cyber actor
- Increased sodium hydroxide level from 100 ppm to 1,100 ppm
- Operator observed the change and corrected dose rate
- Law enforcement notified
- Also was Super Bowl weekend in Tampa

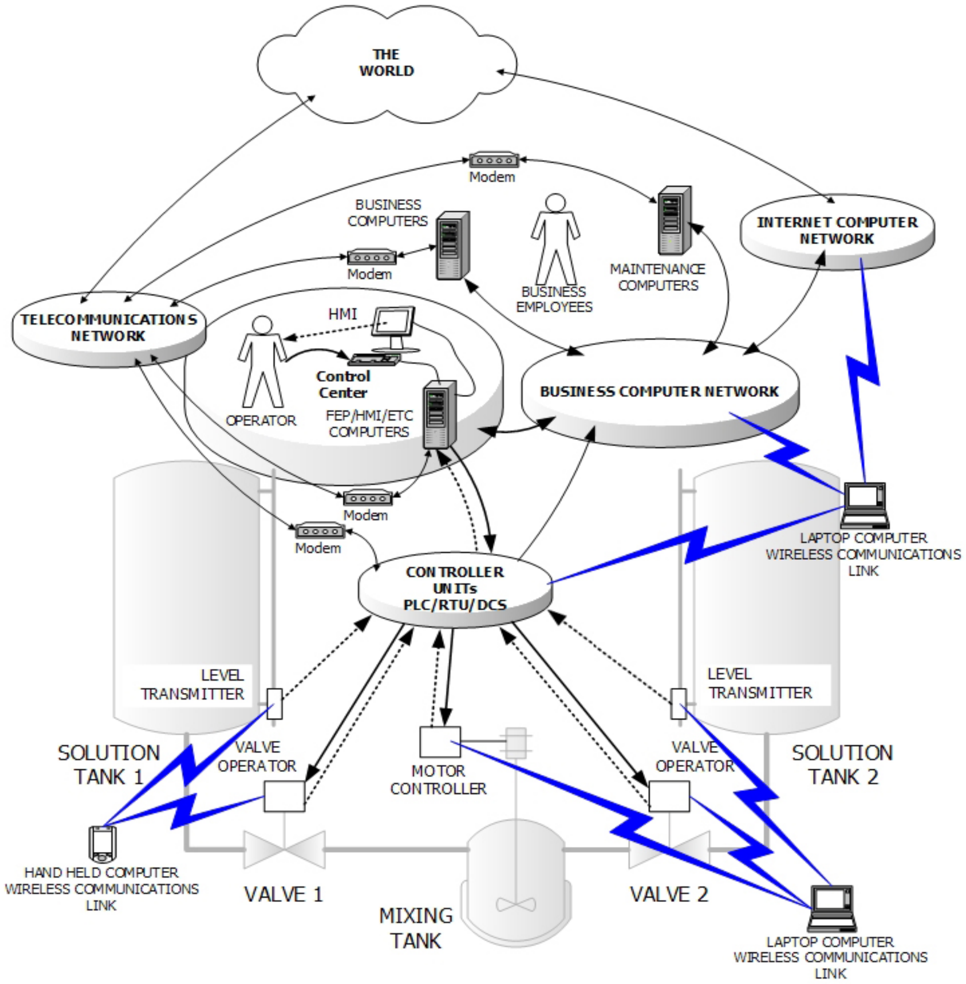
How did it happen?

- Unsecured desktop sharing tool, TeamViewer, was exploited to gain access
- Outdated Windows 7 operating system (support ended Jan 2020)
- Poor password security

Mitigations

- Keep software updated
- Use strong passwords to protect Remote Desktop Protocol (RDP) credentials
- Use multiple factor authentication
- Ensure anti-virus, spam filters, and firewalls are up to date, properly configured, and secure
- Audit network configurations and isolate computer systems that cannot be updated
- Train users to identify and report attempts at social engineering

REALITY: CONNECTIVITY = EXPOSURE



Source: ICS-CERT

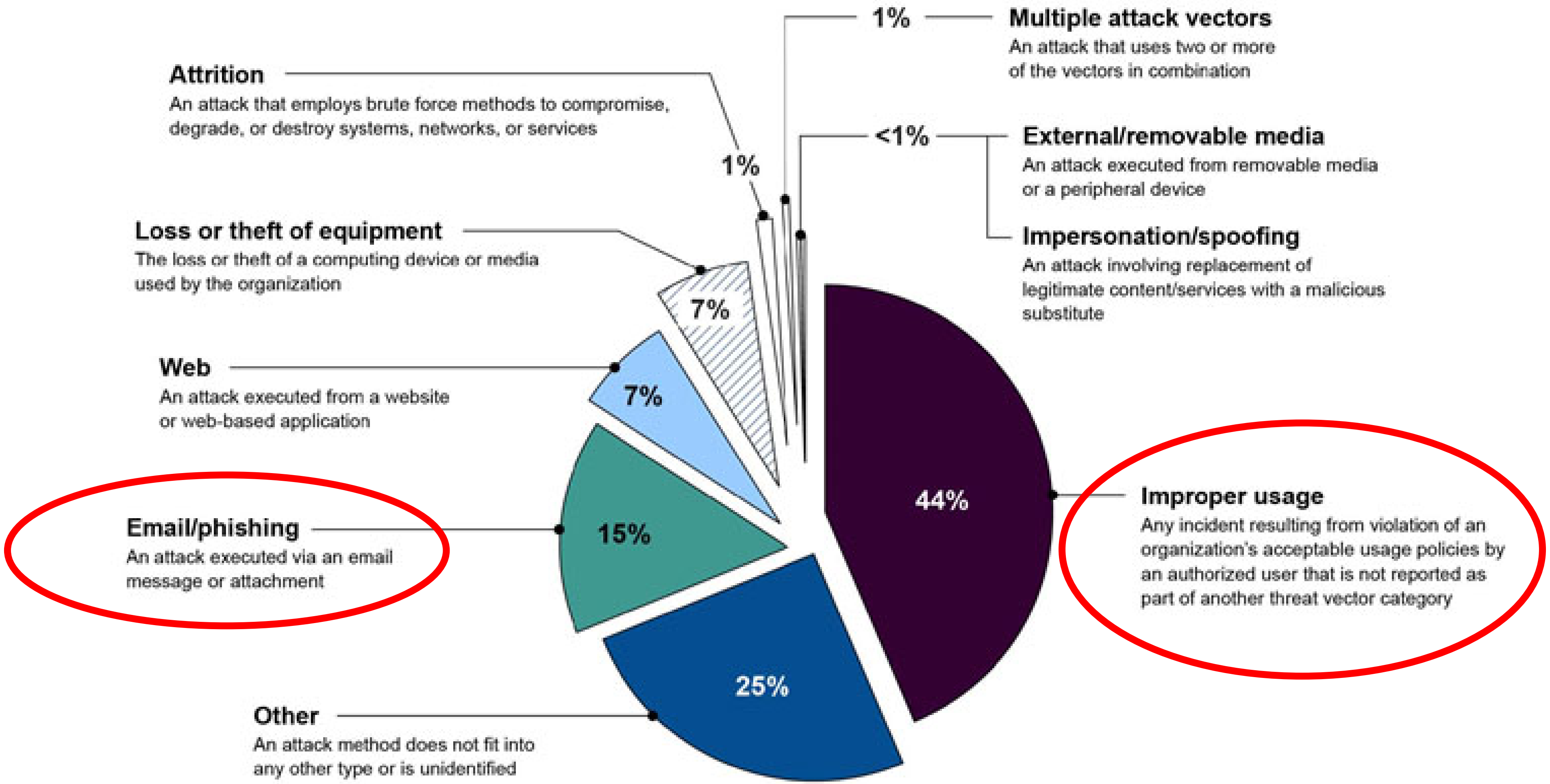
- Enterprise Systems
  - Employee Payroll
  - Service Contracts
  - Customer Billing
  - LIMS etc

- Process Control Systems
  - SCADA
  - AMR/AMI
  - Telecommunications
  - HVAC

PROFILE OF CYBERSECURITY INCIDENTS

US FEDERAL AGENCY SYSTEMS FY19

28,581 total information security incidents



Multiple attack vectors
An attack that uses two or more of the vectors in combination

Attrition
An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services

External/removable media
An attack executed from removable media or a peripheral device

Impersonation/spoofing
An attack involving replacement of legitimate content/services with a malicious substitute

Loss or theft of equipment
The loss or theft of a computing device or media used by the organization

Web
An attack executed from a website or web-based application

Email/phishing
An attack executed via an email message or attachment

Improper usage
Any incident resulting from violation of an organization's acceptable usage policies by an authorized user that is not reported as part of another threat vector category

Other
An attack method does not fit into any other type or is unidentified

Source: GAO analysis of United States Computer Emergency Readiness Team and Office of Management and Budget data for fiscal year 2019.

B. Policy Landscape

KEY DRIVERS FOR CYBERSECURITY

- ***Bioterrorism Act of 2002***
  - Required vulnerability assessment that included threats to *electronic, computer, or other automated systems*

- ***EO 13636: Improving Critical Infrastructure Cybersecurity (Feb 2013)***
  - Charges NIST with creating the Cybersecurity Framework

- ***America's Water Infrastructure Act of 2018, Section 2013***
  - Updates BT Act and <u>expands</u> scope of cyber threat assessment to include:
    - *Monitoring practices of the system, and*
    - *Financial Infrastructure*
  - ERP must include
    - *strategies and resources to improve the resilience of the system*
    - *actions, procedures, and equipment which can obviate or significantly lessen the impact of an incident*

KEY DRIVERS FOR CYBERSECURITY

- **Cyberspace Solarium Commission (2020-21)**
  - Preparing legislative recommendations to enhance cybersecurity across the USG and critical infrastructure; active review of water sector ongoing
- **Department of Homeland Security (2021)**
  - Announced series of cybersecurity “sprints”, which will include actions to improve the resilience of industrial control systems in the water sector.
- **National Security Council (2021)**
  - Developing a plan to address “integrity” of industrial control systems in the water and power sectors.
- **S. 914 -** Drinking Water and Wastewater Infrastructure Act of2021
  - Create prioritized framework by EPA and DHS

America’s Water Infrastructure Act of 2018, §2013#

Community Water System (pop. served)*	Certify Risk & Resilience Assessment (RRA) prior to:	Certify ERP within 6 months of RRA, but not later than:
>100K	✓ March 31, 2020	✓ September 30, 2020
50,000 – 99,999	✓ December 31, 2020	June 30, 2021
3,300 – 49,999	June 30, 2021	December 30, 2021

*** Wholesalers use pop of all systems**

# Must review, update & recertify every 5 years

What must a Utility Assess?

The Risks to, and Resilience of, its system considering:

- **malevolent acts and natural hazards**;
- resilience of the pipes and constructed conveyances, physical barriers, **source water**, water collection and intake, pretreatment, treatment, storage and distribution facilities, electronic, computer, or other automated systems;
- **the monitoring practices of the system;**
- **the financial infrastructure of the system**;
- the use, storage, or handling of various chemicals by the system; and
- the operation and maintenance of the system; and
- **may include an evaluation of capital and operational needs for risk and resilience management.**

Definitions (*not specified in statute*)

- ***Monitoring practices of the system*** means any systems that the utility uses to monitor operations such as water quality, security surveillance systems, access control systems, cyber security systems, energy management systems, or others.

- ***Financial Infrastructure*** means the accounting and financial business systems operated by a utility, such as customer billing and payment systems that may be vulnerable to cybersecurity threats.

What must the ERP include?

- ***strategies and resources to improve the resilience of the system, including the physical security and cybersecurity of the system***;

- plans and procedures that can be implemented, and identification of equipment that can be utilized, in the event of a ***malevolent act or natural hazard that threatens the ability of the community water system to deliver safe drinking water***;

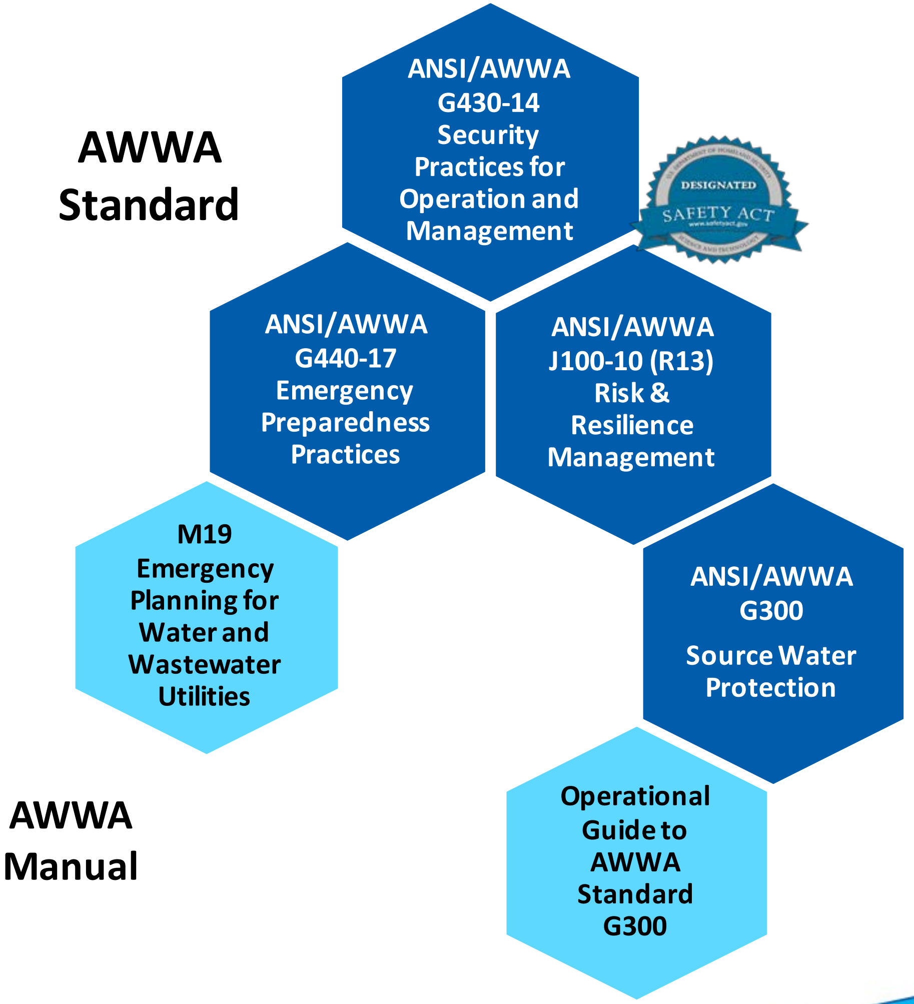
- actions, procedures, and equipment which can obviate or significantly lessen the impact of ***a malevolent act or natural hazard*** on the public health and the safety and supply of drinking water provided to communities and individuals, ***including the development of alternative source water options, relocation of water intakes, and construction of flood protection barriers***; and

- ***strategies that can be used to aid in the detection of malevolent acts or natural hazards that threaten the security or resilience of the system***.

C. Water Sector Approach

RISK & RESILIENCE ⇔ ALL-HAZARDS APPROACH

AWWA RISK & RESILIENCE RESOURCE SUITE



AWWA Standard

ANSI/AWWA G430-14 Security Practices for Operation and Management

ANSI/AWWA G440-17 Emergency Preparedness Practices

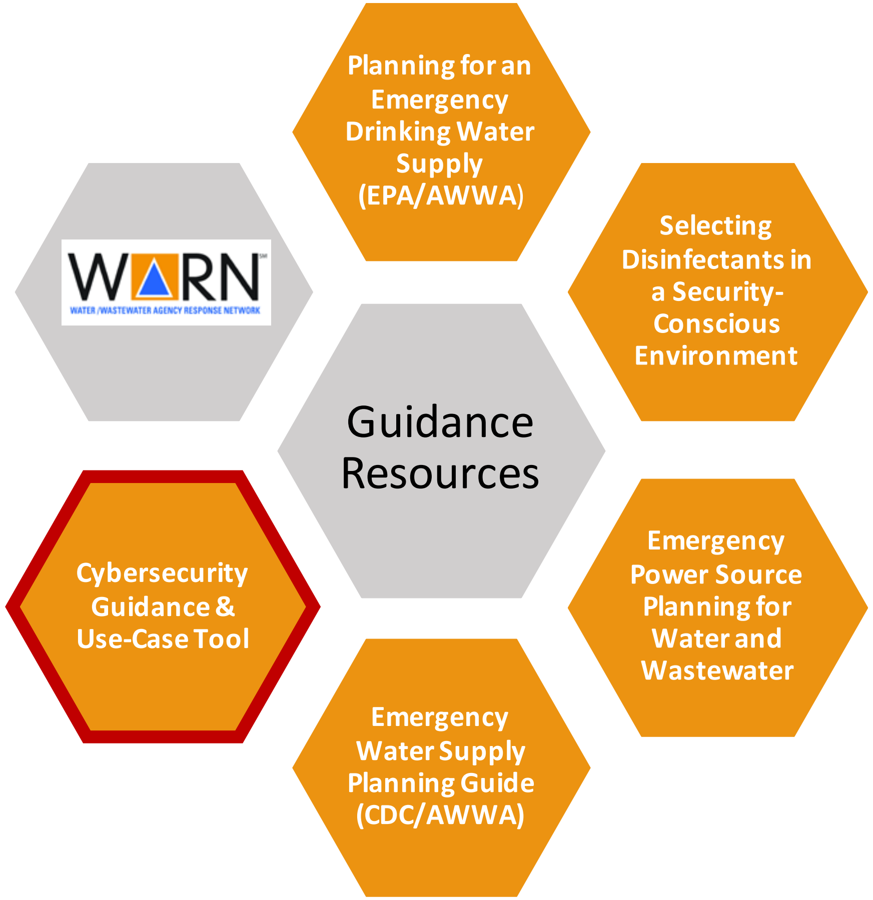
ANSI/AWWA J100-10 (R13) Risk & Resilience Management

ANSI/AWWA G300 Source Water Protection

AWWA Manual

M19 Emergency Planning for Water and Wastewater Utilities

Operational Guide to AWWA Standard G300



Guidance Resources

Planning for an Emergency Drinking Water Supply (EPA/AWWA)

Selecting Disinfectants in a Security-Conscious Environment

Emergency Power Source Planning for Water and Wastewater

Emergency Water Supply Planning Guide (CDC/AWWA)

Cybersecurity Guidance & Use-Case Tool

FOUNDATION FOR DUE DILIGENCE

DESIGNATED SAFETY ACT

ANSI/AWWA G430: Security Practices for Operation & Management

- Information protection and continuity is a requirement

DESIGNATED SAFETY ACT

ANSI/AWWA J100: Risk & Resilience Management of Water & Wastewater Systems

- Cyber is required threat domain

ANSI/AWWA G440: Emergency Preparedness Practices

- Consideration of key business & operating system recovery

Cybersecurity Risk & Responsibility in the Water Sector

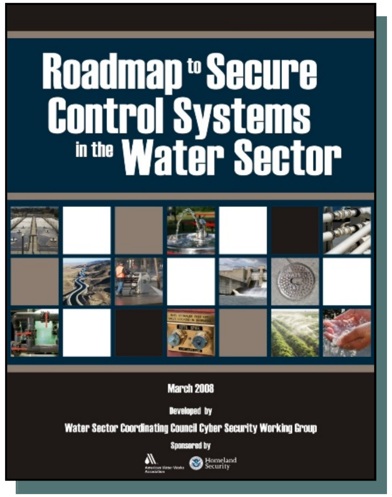
- Utility has fiduciary responsibility to manage cyber risks

Water Sector Cybersecurity Risk Management Guidance

- Supports voluntary adoption of NIST Cybersecurity Framework
- Addresses cyber provision in AWIA §2013

WATER SECTOR & CYBERSECURITY

- **Y2K**
- **BT Act 2002**



Roadmap to Secure Control Systems in the Water Sector

March 2008

Developed by

Water Sector Coordinating Council Cyber Security Working Group

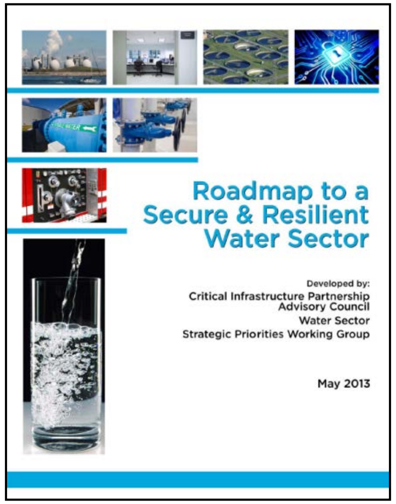
Sponsored by

American Water Works Association

Homeland Security

<u>2008 Critical Milestone</u>

Develop a recommended practices ICS security template for widespread use in the water sector



Roadmap to a Secure & Resilient Water Sector

Developed by:

Critical Infrastructure Partnership Advisory Council

Water Sector

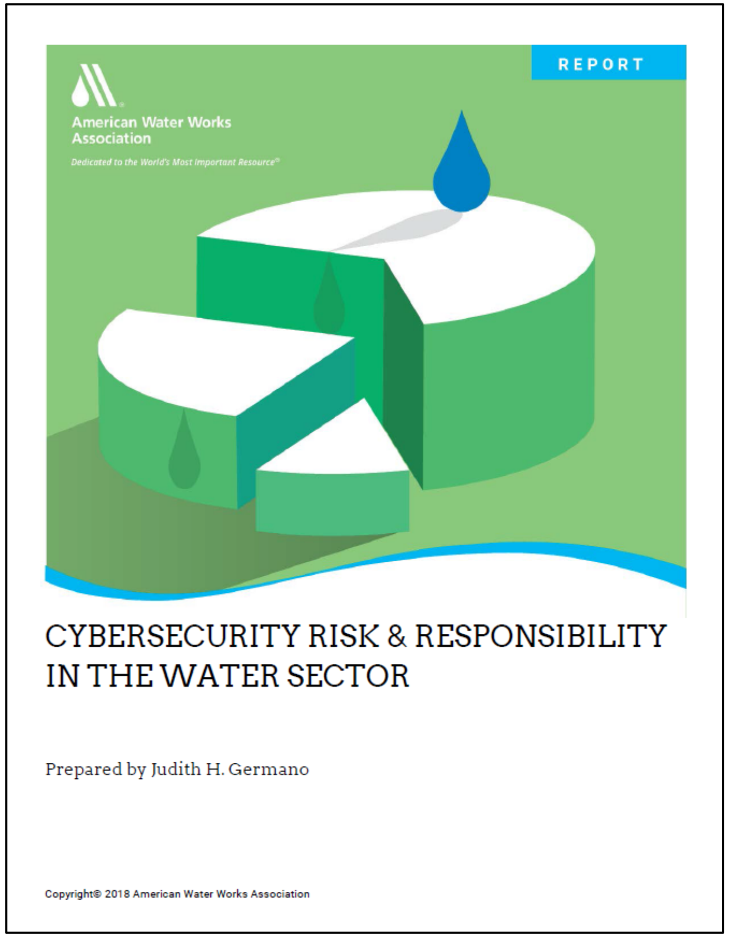
Strategic Priorities Working Group

May 2013

<u>2013 & 2017 #1 Priority</u>

Advance the development of sector-specific cybersecurity resources

CYBERSECURITY RISK & RESPONSIBILITY



REPORT

American Water Works Association

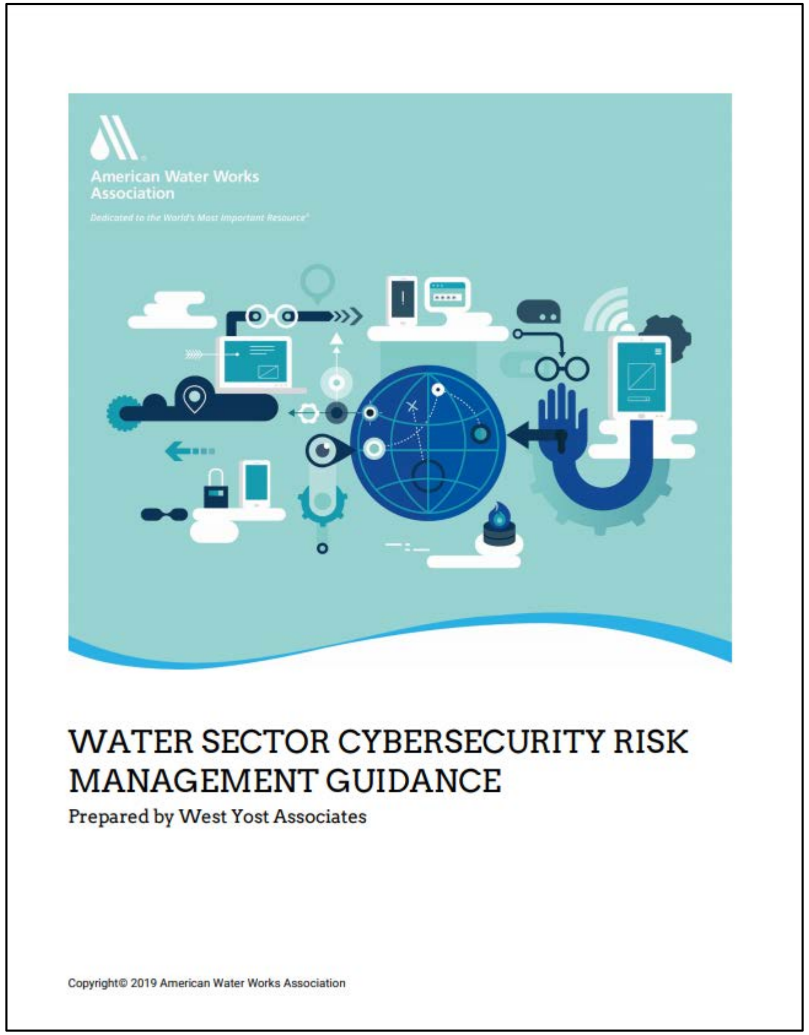
Dedicated to the World's Most Important Resource®

CYBERSECURITY RISK & RESPONSIBILITY
IN THE WATER SECTOR

Prepared by Judith H. Germano

- Cyber Threats are Foreseeable
- Implement Best Practices
- Demonstrate Due Diligence
- Insurance provides some risk transfer
- Sovereign Immunity is not option
- ***Fiduciary Responsibility***

IMPLEMENTING BEST PRACTICE



American Water Works Association

Dedicated to the World's Most Important Resource®

WATER SECTOR CYBERSECURITY RISK MANAGEMENT GUIDANCE

Prepared by West Yost Associates

- **Recognized by USEPA, DHS, NIST and multiple states**.

- Provides a consistent and repeatable recommended course of action to reduce vulnerabilities in process control systems.

- Fulfills need for sector-specific guidance as specified in EO 13636, and aligns with national priorities.

14 CORE PRACTICE CATEGORIES

Governance & Risk Management

Business Continuity

Server and Workstation Hardening

Access Control

Application Security

Encryption

Telecom, Network Security, & Architecture

Physical Security of PCS Equipment

Service Level Agreements

Operations Security

Education

Personnel Security

Supply Chain

Cyber Informed Engineering

The Self-Assessment Questionnaire – Example

1. Are any data transferred to or from your Process Control System network, by any electronic means?

Additional Details:

- Examples of electronic data transfer include both automatic (e.g. automated export of data from the PCS environment) and manual (e.g. transfer of data to/from the PCS environment via thumb drive). Examples of data that may be transferred include:
  - Water quality data collected by the PCS and transferred for regulatory reporting
  - Asset performance data for asset management
  - Operating system/software patches and updates

❑ Yes

❑ No

AWWA Tool Controls

Controls are based on standards published by the following agencies:

- AWWA
- DHS
- IEC
- INL
- ISA
- ISO
- NIST
- PCI DSS

Control Recommendation Priorities

Priority 1: IMPLEMENT IMMEDIATELY

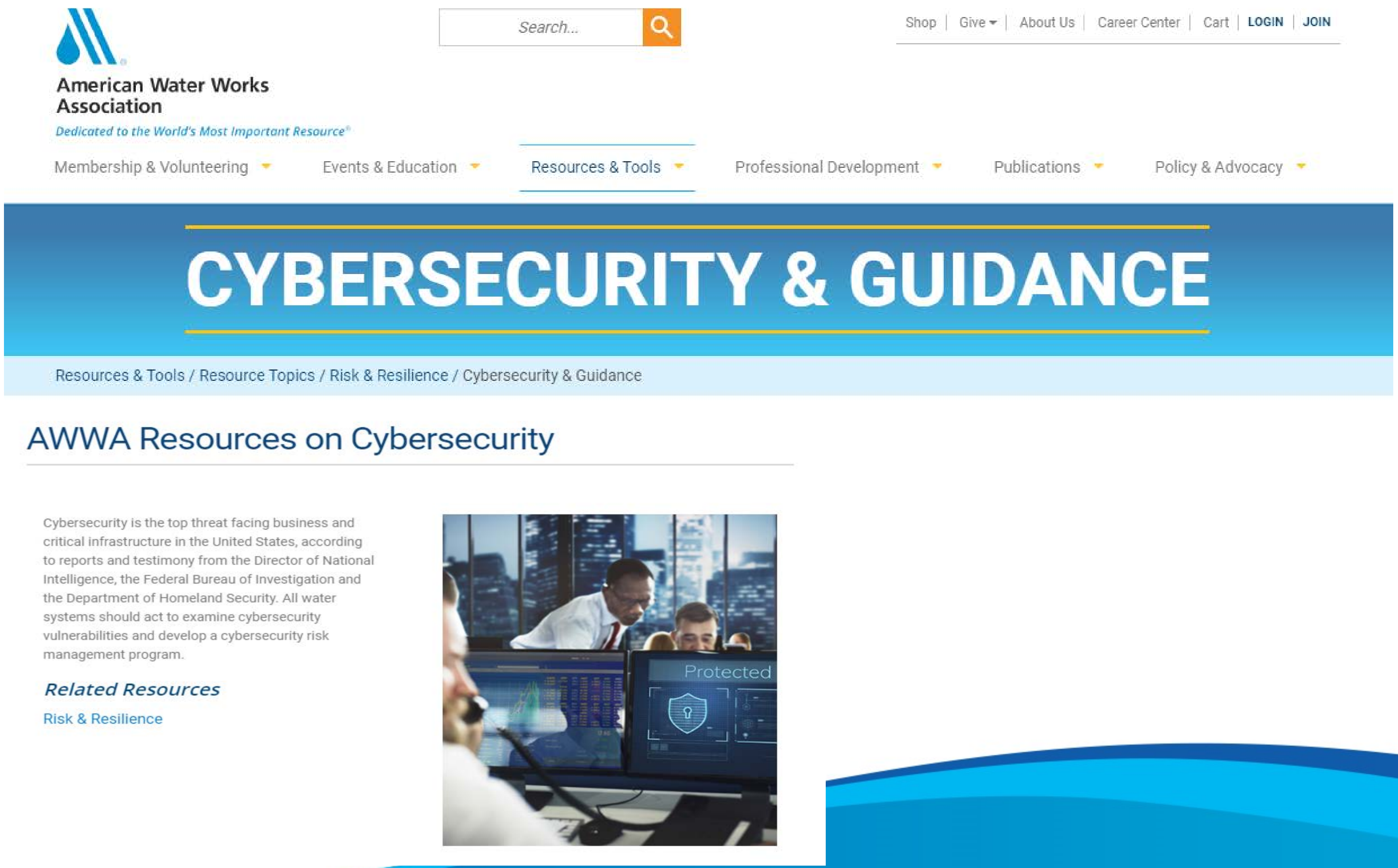
Priority 2: Significant increase in security of organization

Priority 3: Foundation for managed security system

Priority 4: Protection for sophisticated, but less common attacks

HOW DO YOU USE THE AWWA CYBERSECURITY ASSESSMENT TOOL?

Step 1 – Go to www.awwa.org/cybersecurity


American Water Works Association
Dedicated to the World's Most Important Resource®
Search...
Shop | Give | About Us | Career Center | Cart | LOGIN | JOIN
Membership & Volunteering
Events & Education
Resources & Tools
Professional Development
Publications
Policy & Advocacy
Resources & Tools / Resource Topics / Risk & Resilience / Cybersecurity & Guidance
Protected

CYBERSECURITY & GUIDANCE

AWWA Resources on Cybersecurity

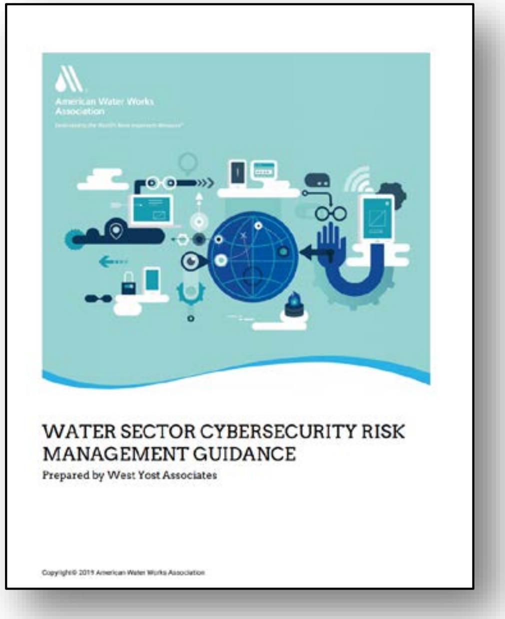
Cybersecurity is the top threat facing business and critical infrastructure in the United States, according to reports and testimony from the Director of National Intelligence, the Federal Bureau of Investigation and the Department of Homeland Security. All water systems should act to examine cybersecurity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

Related Resources

Risk & Resilience

Step 2 – Answer the Self-Assessment Questionnaire

A. *Read* the guidance!



American Water Works Association

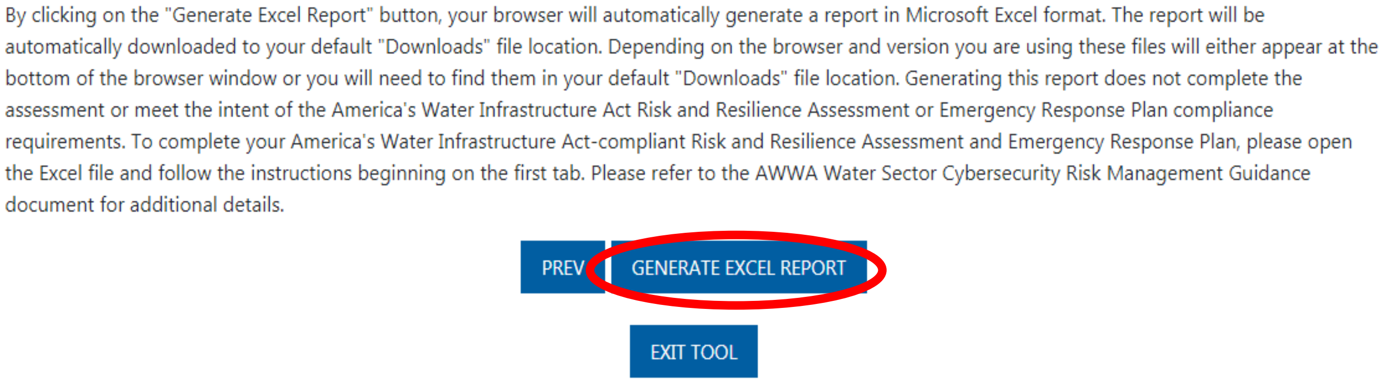
WATER SECTOR CYBERSECURITY RISK MANAGEMENT GUIDANCE

Prepared by West Yost Associates

Copyright© 2019 American Water Works Association

B. *Answer 22 total questions*

C. *Generate your output file including recommended controls*



By clicking on the "Generate Excel Report" button, your browser will automatically generate a report in Microsoft Excel format. The report will be automatically downloaded to your default "Downloads" file location. Depending on the browser and version you are using these files will either appear at the bottom of the browser window or you will need to find them in your default "Downloads" file location. Generating this report does not complete the assessment or meet the intent of the America's Water Infrastructure Act Risk and Resilience Assessment or Emergency Response Plan compliance requirements. To complete your America's Water Infrastructure Act-compliant Risk and Resilience Assessment and Emergency Response Plan, please open the Excel file and follow the instructions beginning on the first tab. Please refer to the AWWA Water Sector Cybersecurity Risk Management Guidance document for additional details.

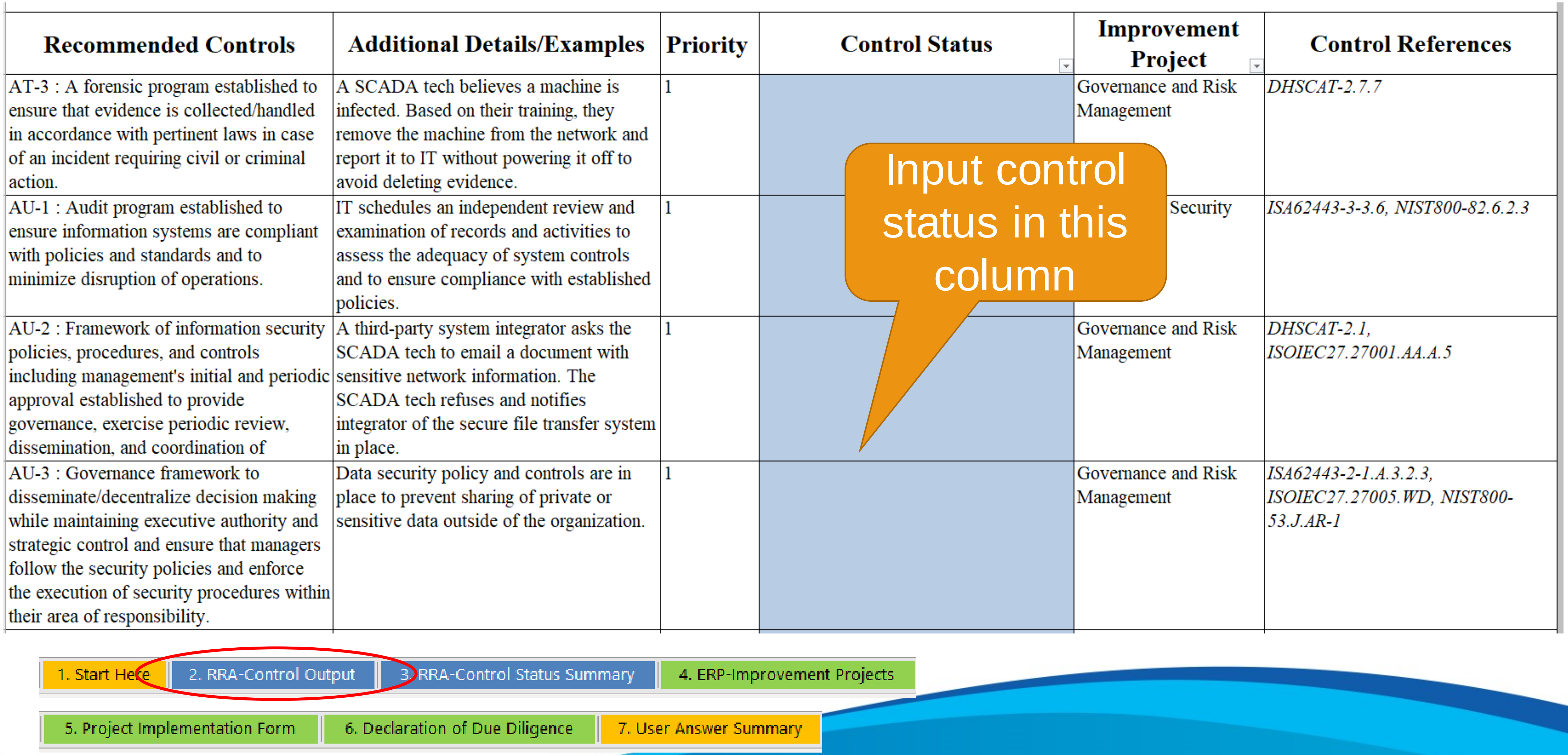
Tool Output – What is it? What isn’t it?

- ✓List of recommended, prioritized controls based on user to the Self-Assessment Questionnaire
- ✓Great start to an AWIA-compliant RRA & ERP

- ✓The Tool does not *automatically* assess which recommended controls the utility may already have in place
- ✓The Tool does not provide specific information on how a recommended control should be implemented

Completion of the Self-Assessment Questionnaire does not provide AWIA compliance

Step 3 – Determine Control Status



Recommended Controls	Additional Details/Examples	Priority	Control Status	Improvement Project	Control References
AT-3 : A forensic program established to ensure that evidence is collected/handled in accordance with pertinent laws in case of an incident requiring civil or criminal action.	A SCADA tech believes a machine is infected. Based on their training, they remove the machine from the network and report it to IT without powering it off to avoid deleting evidence.	1		Governance and Risk Management	*DHSCAT-2.7.7*
AU-1 : Audit program established to ensure information systems are compliant with policies and standards and to minimize disruption of operations.	IT schedules an independent review and examination of records and activities to assess the adequacy of system controls and to ensure compliance with established policies.	1		Security	*ISA62443-3-3.6, NIST800-82.6.2.3*
AU-2 : Framework of information security policies, procedures, and controls including management's initial and periodic approval established to provide governance, exercise periodic review, dissemination, and coordination of	A third-party system integrator asks the SCADA tech to email a document with sensitive network information. The SCADA tech refuses and notifies integrator of the secure file transfer system in place.	1		Governance and Risk Management	*DHSCAT-2.1, ISOIEC27.27001.AA.A.5*
AU-3 : Governance framework to disseminate/decentralize decision making while maintaining executive authority and strategic control and ensure that managers follow the security policies and enforce the execution of security procedures within their area of responsibility.	Data security policy and controls are in place to prevent sharing of private or sensitive data outside of the organization.	1		Governance and Risk Management	*ISA62443-2-1.A.3.2.3, ISOIEC27.27005.WD, NIST800-53.J.AR-1*

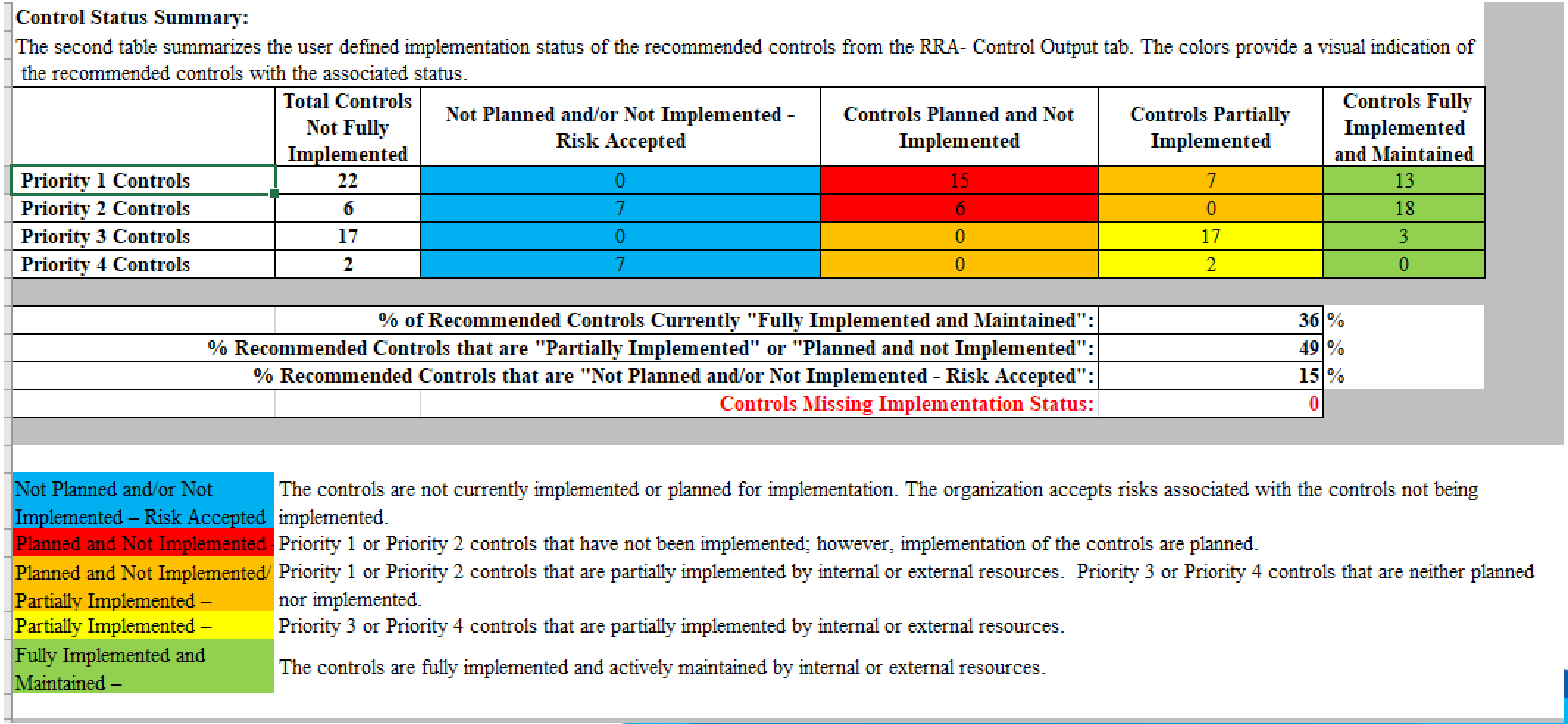
1. Start Here
2. RRA-Control Output
3. RRA-Control Status Summary
4. ERP-Improvement Projects
5. Project Implementation Form
6. Declaration of Due Diligence
7. User Answer Summary

Input control status in this column

Control Status Options

1. **Not Planned and/or Not Implemented – Risk Accepted** – The controls are not currently implemented or planned for implementation. The organization accepts risks associated with the controls not being implemented.
2. **Planned and Not Implemented** – The controls is currently planned for future implementation.
3. **Partially Implemented** – The controls are partially implemented by internal or external resources.
4. **Fully Implemented and Maintained** – The controls are fully implemented and actively maintained by internal or external resources.

STATUS CHECK & DUE DILIGENCE



Control Status Summary:

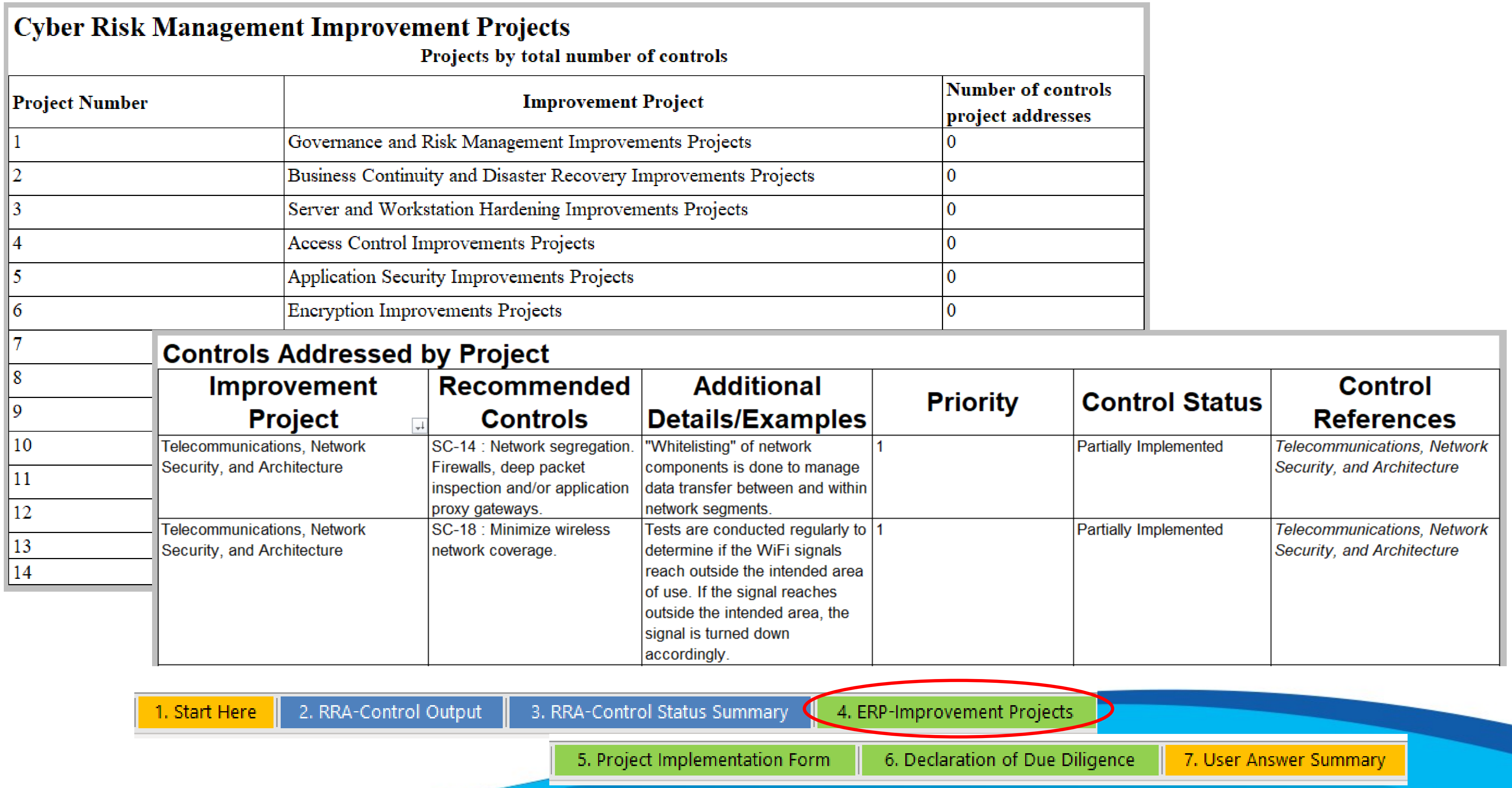
The second table summarizes the user defined implementation status of the recommended controls from the RRA- Control Output tab. The colors provide a visual indication of the recommended controls with the associated status.

	Total Controls Not Fully Implemented	Not Planned and/or Not Implemented - Risk Accepted	Controls Planned and Not Implemented	Controls Partially Implemented	Controls Fully Implemented and Maintained
Priority 1 Controls	22	0	15	7	13
Priority 2 Controls	6	7	6	0	18
Priority 3 Controls	17	0	0	17	3
Priority 4 Controls	2	7	0	2	0

% of Recommended Controls Currently "Fully Implemented and Maintained":	36	%
% Recommended Controls that are "Partially Implemented" or "Planned and not Implemented":	49	%
% Recommended Controls that are "Not Planned and/or Not Implemented - Risk Accepted":	15	%
Controls Missing Implementation Status:	0	

Not Planned and/or Not Implemented – Risk Accepted	The controls are not currently implemented or planned for implementation. The organization accepts risks associated with the controls not being implemented.
Planned and Not Implemented	Priority 1 or Priority 2 controls that have not been implemented; however, implementation of the controls are planned.
Planned and Not Implemented/ Partially Implemented –	Priority 1 or Priority 2 controls that are partially implemented by internal or external resources. Priority 3 or Priority 4 controls that are neither planned nor implemented.
Partially Implemented –	Priority 3 or Priority 4 controls that are partially implemented by internal or external resources.
Fully Implemented and Maintained –	The controls are fully implemented and actively maintained by internal or external resources.

Step 4 – Design Improvement Projects



Cyber Risk Management Improvement Projects

Projects by total number of controls

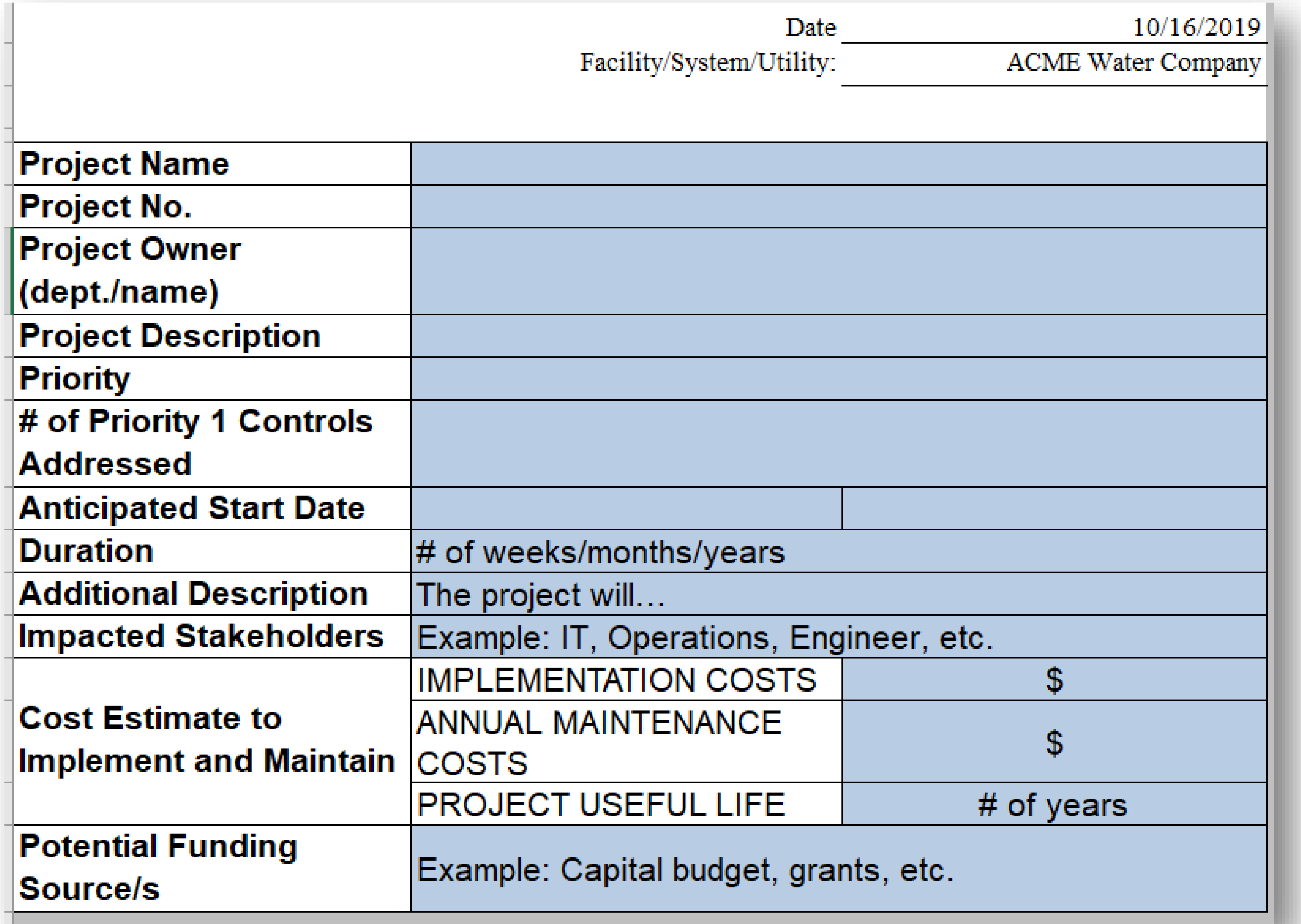
Project Number	Improvement Project	Number of controls project addresses
1	Governance and Risk Management Improvements Projects	0
2	Business Continuity and Disaster Recovery Improvements Projects	0
3	Server and Workstation Hardening Improvements Projects	0
4	Access Control Improvements Projects	0
5	Application Security Improvements Projects	0
6	Encryption Improvements Projects	0
7		
8		
9		
10		
11		
12		
13		
14		

Controls Addressed by Project

Improvement Project	Recommended Controls	Additional Details/Examples	Priority	Control Status	Control References
Telecommunications, Network Security, and Architecture	SC-14 : Network segregation. Firewalls, deep packet inspection and/or application proxy gateways.	"Whitelisting" of network components is done to manage data transfer between and within network segments.	1	Partially Implemented	*Telecommunications, Network Security, and Architecture*
Telecommunications, Network Security, and Architecture	SC-18 : Minimize wireless network coverage.	Tests are conducted regularly to determine if the WiFi signals reach outside the intended area of use. If the signal reaches outside the intended area, the signal is turned down accordingly.	1	Partially Implemented	*Telecommunications, Network Security, and Architecture*

1. Start Here
2. RRA-Control Output
3. RRA-Control Status Summary
4. ERP-Improvement Projects
5. Project Implementation Form
6. Declaration of Due Diligence
7. User Answer Summary

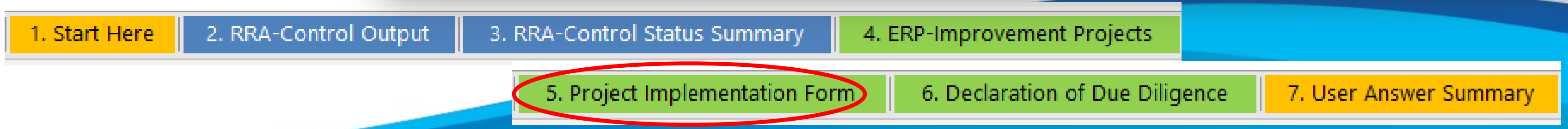
OPTIONAL Step 5 – Project Implementation Form



Date 10/16/2019

Facility/System/Utility: ACME Water Company

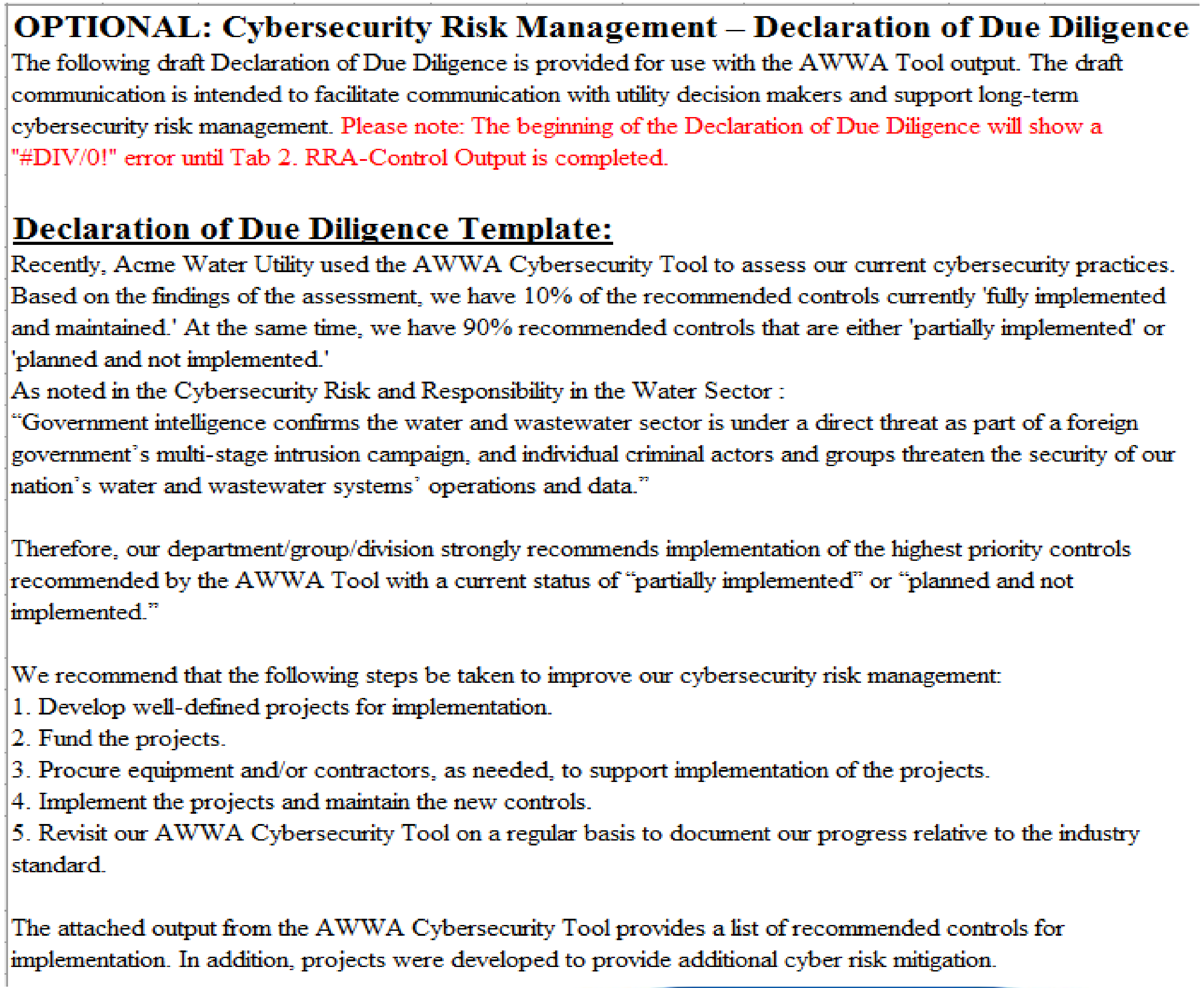
Project Name		
Project No.		
Project Owner (dept./name)		
Project Description		
Priority		
# of Priority 1 Controls Addressed		
Anticipated Start Date		
Duration	# of weeks/months/years	
Additional Description	The project will…	
Impacted Stakeholders	Example: IT, Operations, Engineer, etc.	
Cost Estimate to Implement and Maintain	IMPLEMENTATION COSTS	$
	ANNUAL MAINTENANCE COSTS	$
	PROJECT USEFUL LIFE	# of years
Potential Funding Source/s	Example: Capital budget, grants, etc.	



1. Start Here | 2. RRA-Control Output | 3. RRA-Control Status Summary | 4. ERP-Improvement Projects

5. Project Implementation Form | 6. Declaration of Due Diligence | 7. User Answer Summary

OPTIONAL Step 6: Declaration of Due Diligence



OPTIONAL: Cybersecurity Risk Management – Declaration of Due Diligence

The following draft Declaration of Due Diligence is provided for use with the AWWA Tool output. The draft communication is intended to facilitate communication with utility decision makers and support long-term cybersecurity risk management. Please note: The beginning of the Declaration of Due Diligence will show a "#DIV/0!" error until Tab 2. RRA-Control Output is completed.

Declaration of Due Diligence Template:

Recently, Acme Water Utility used the AWWA Cybersecurity Tool to assess our current cybersecurity practices. Based on the findings of the assessment, we have 10% of the recommended controls currently 'fully implemented and maintained.' At the same time, we have 90% recommended controls that are either 'partially implemented' or 'planned and not implemented.'

As noted in the Cybersecurity Risk and Responsibility in the Water Sector :

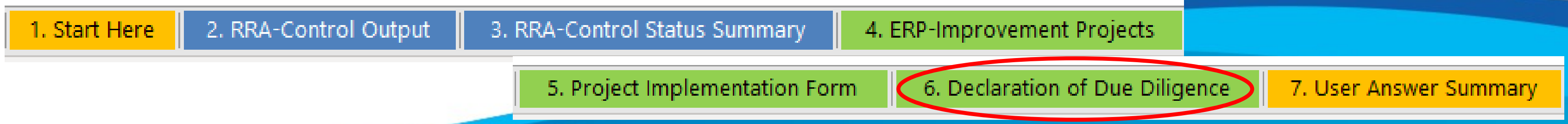
"Government intelligence confirms the water and wastewater sector is under a direct threat as part of a foreign government's multi-stage intrusion campaign, and individual criminal actors and groups threaten the security of our nation's water and wastewater systems' operations and data."

Therefore, our department/group/division strongly recommends implementation of the highest priority controls recommended by the AWWA Tool with a current status of "partially implemented" or "planned and not implemented."

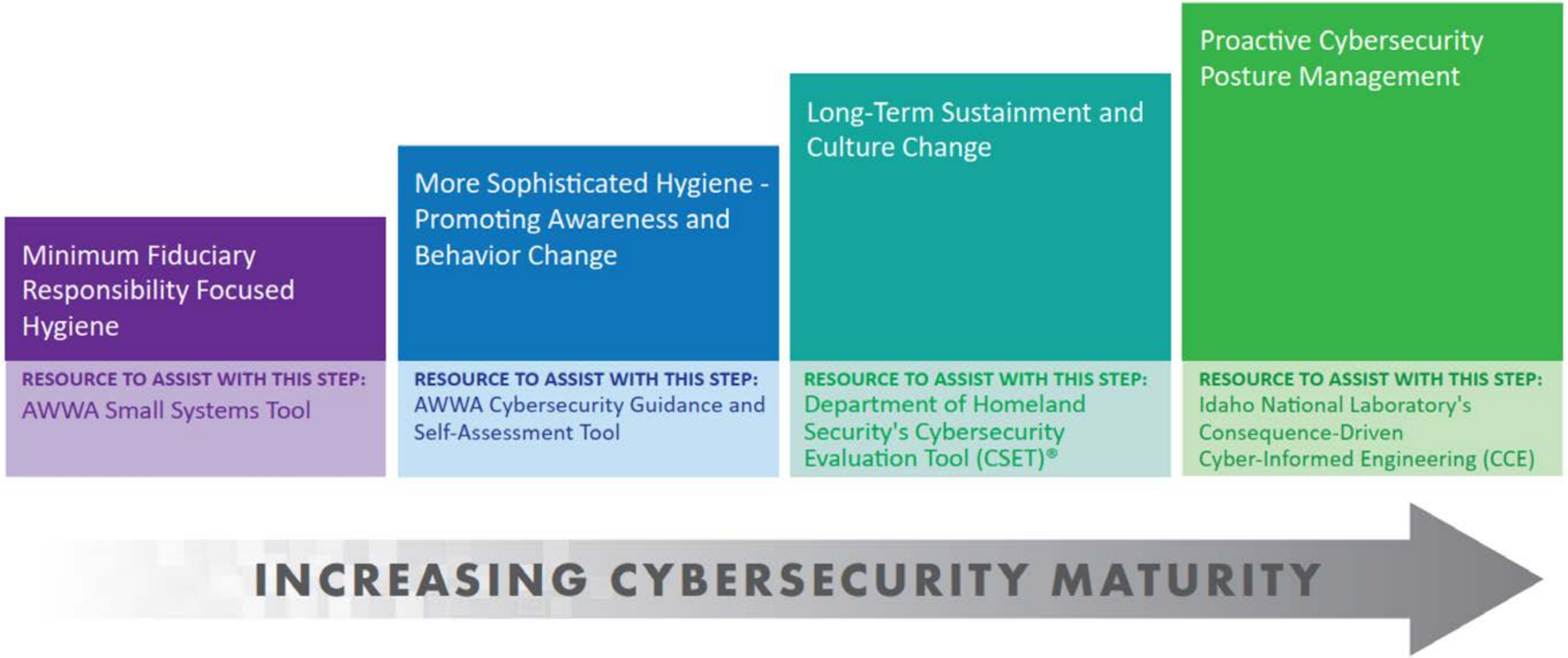
We recommend that the following steps be taken to improve our cybersecurity risk management:

1. Develop well-defined projects for implementation.
2. Fund the projects.
3. Procure equipment and/or contractors, as needed, to support implementation of the projects.
4. Implement the projects and maintain the new controls.
5. Revisit our AWWA Cybersecurity Tool on a regular basis to document our progress relative to the industry standard.

The attached output from the AWWA Cybersecurity Tool provides a list of recommended controls for implementation. In addition, projects were developed to provide additional cyber risk mitigation.


1. Start Here
2. RRA-Control Output
3. RRA-Control Status Summary
4. ERP-Improvement Projects
5. Project Implementation Form
6. Declaration of Due Diligence
7. User Answer Summary

THE GOAL – PROGRESS ON CYBERSECURITY PRACTICES



Minimum Fiduciary Responsibility Focused Hygiene

RESOURCE TO ASSIST WITH THIS STEP:
AWWA Small Systems Tool

More Sophisticated Hygiene - Promoting Awareness and Behavior Change

RESOURCE TO ASSIST WITH THIS STEP:
AWWA Cybersecurity Guidance and Self-Assessment Tool

Long-Term Sustainment and Culture Change

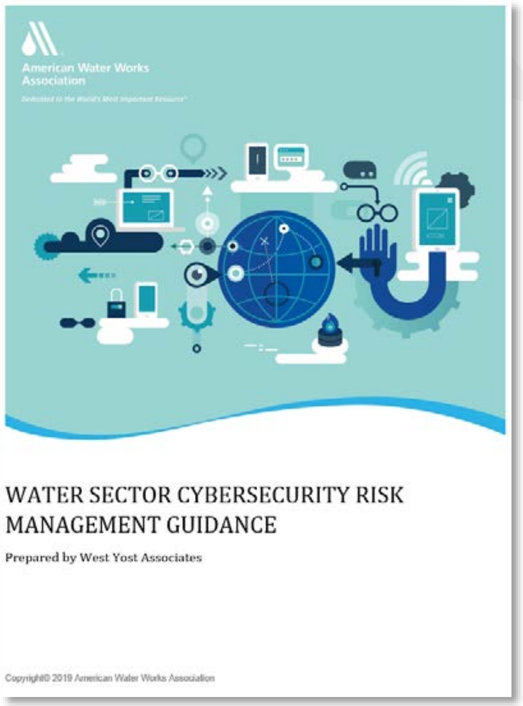
RESOURCE TO ASSIST WITH THIS STEP:
Department of Homeland Security's Cybersecurity Evaluation Tool (CSET)®

Proactive Cybersecurity Posture Management

RESOURCE TO ASSIST WITH THIS STEP:
Idaho National Laboratory's Consequence-Driven Cyber-Informed Engineering (CCE)

INCREASING CYBERSECURITY MATURITY

Adopted from SANS.org.



American Water Works Association

Dedicated to the World's Most Important Resource®

WATER SECTOR CYBERSECURITY RISK MANAGEMENT GUIDANCE

Prepared by West Yost Associates

Key Incident Response Contacts

Federal Bureau of Investigation (FBI)

FBI Field Office Cyber Task Forces:
http://www.fbi.gov/contact-us/field

Internet Crime Complaint Center (IC3)
http://www.ic3.gov

National Cyber Investigative Joint Task Force

NCIJTF CyWatch 24/7 Command Center:
(855) 292-3937 or cywatch@ic.fbi.gov

National Cybersecurity and Communications Integration Center (NCCIC)

NCCIC: (888) 282-0870 or NCCIC@hq.dhs.gov

United States Computer Emergency Readiness Team:
http://www.us-cert.gov

State Fusion Center

State and major urban area fusion centers (fusion centers) are owned and operated by state and local entities, and are designated by the governor of their state.

https://www.dhs.gov/fusion-center-locations-and-contact-information

Questions

Kevin M. Morley, PhD

Manager, Federal Relations
AWWA – Government Affairs
202-628-8303 or kmorley@awwa.org

www.awwa.org/risk
www.awwa.org/cybersecurity