Operational Technology Cybersecurity

Several Cybersecurity Topics Currently Affecting Water & Wastewater Utilities

April 10, 2023

Jim Schultz
Laurie Kusmaul

Presenters

Jim Schultz

PE (PA), CISSP, CISA, CCNA, C|EH , GICSP

Sr. OT Cybersecurity Consultant

Laurie Kusmaul

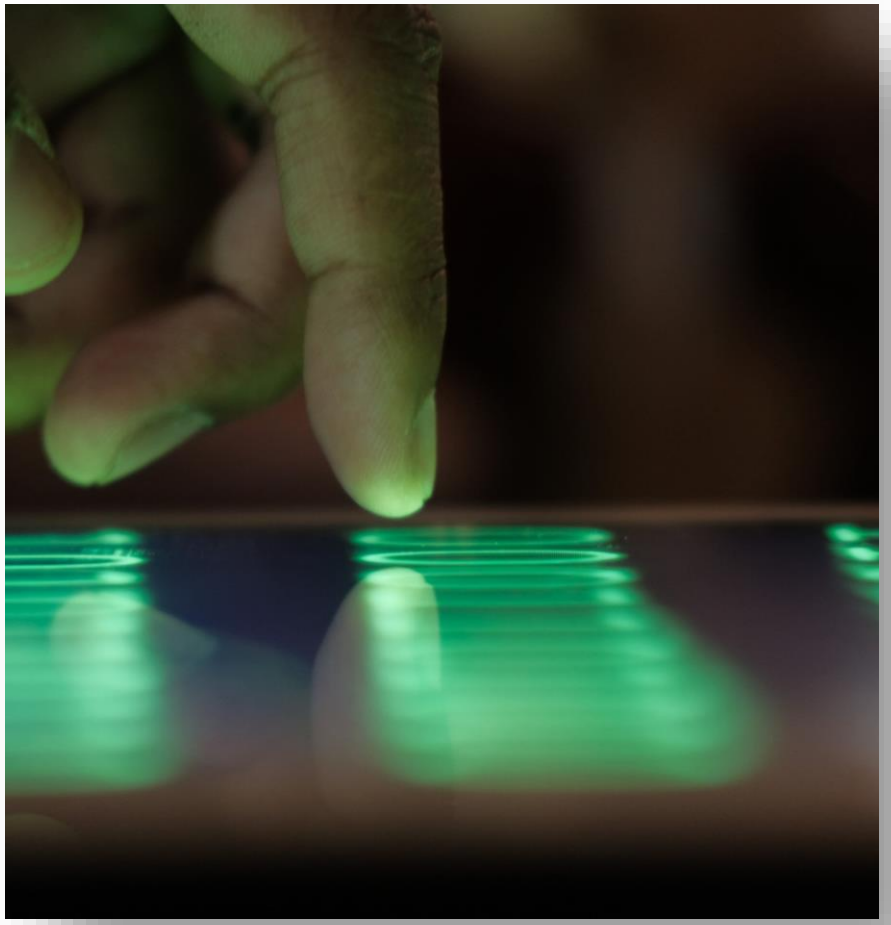
MISM, Information Security

Control System Programmer

OT Cybersecurity Consultant

Today's Agenda

- Getting in Sync
- Current State of Cybersecurity
  - History of W/WW Cyber Attacks
  - FL State IT/OT Cyber Mandate
  - Federal EPA Water-Cyber Mandate
  - American Water Infrastructure Act (AWIA) of 2018
- Getting Started
  - Key Concepts
  - Easy Ways to Reduce Risk



1 Getting in Sync

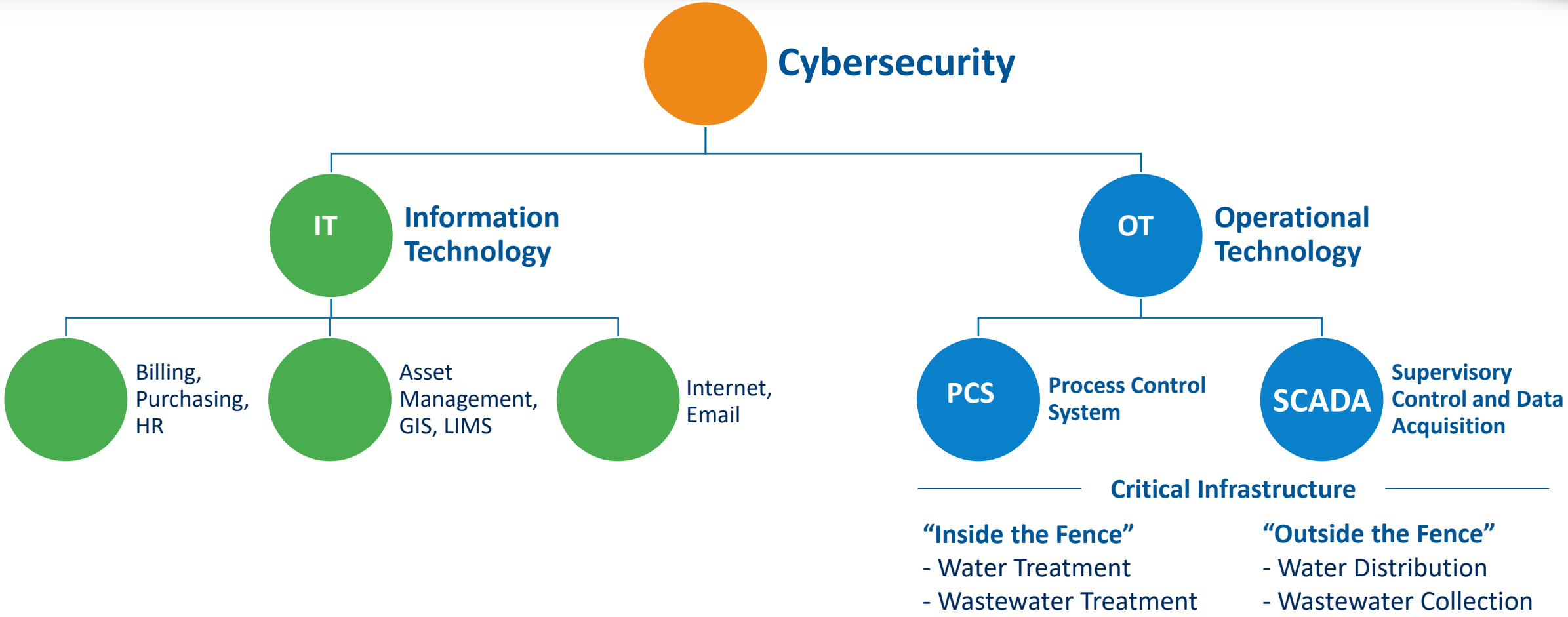
Getting in Sync - Terminology

- Control Systems
  - **Controls**
    - PLCs
    - Single loop controllers
    - Relays
    - Pushbuttons
    - etc.

- Cybersecurity
  - **Controls**
    - Multifactor Authentication
    - Network segmentation
    - Backups
    - Training
    - etc.

When you hear "controls" in a cyber discussion . . . think "countermeasures."

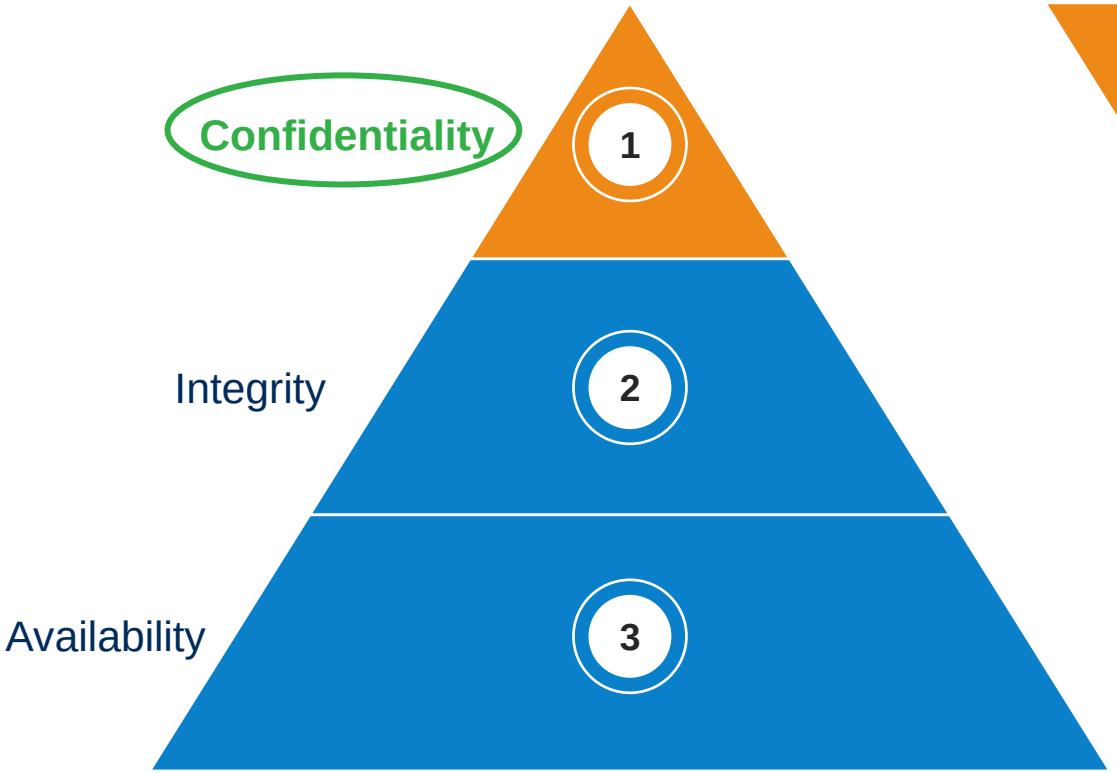
Getting in Sync - Terminology



When you hear "OT" . . . think "critical infrastructure."

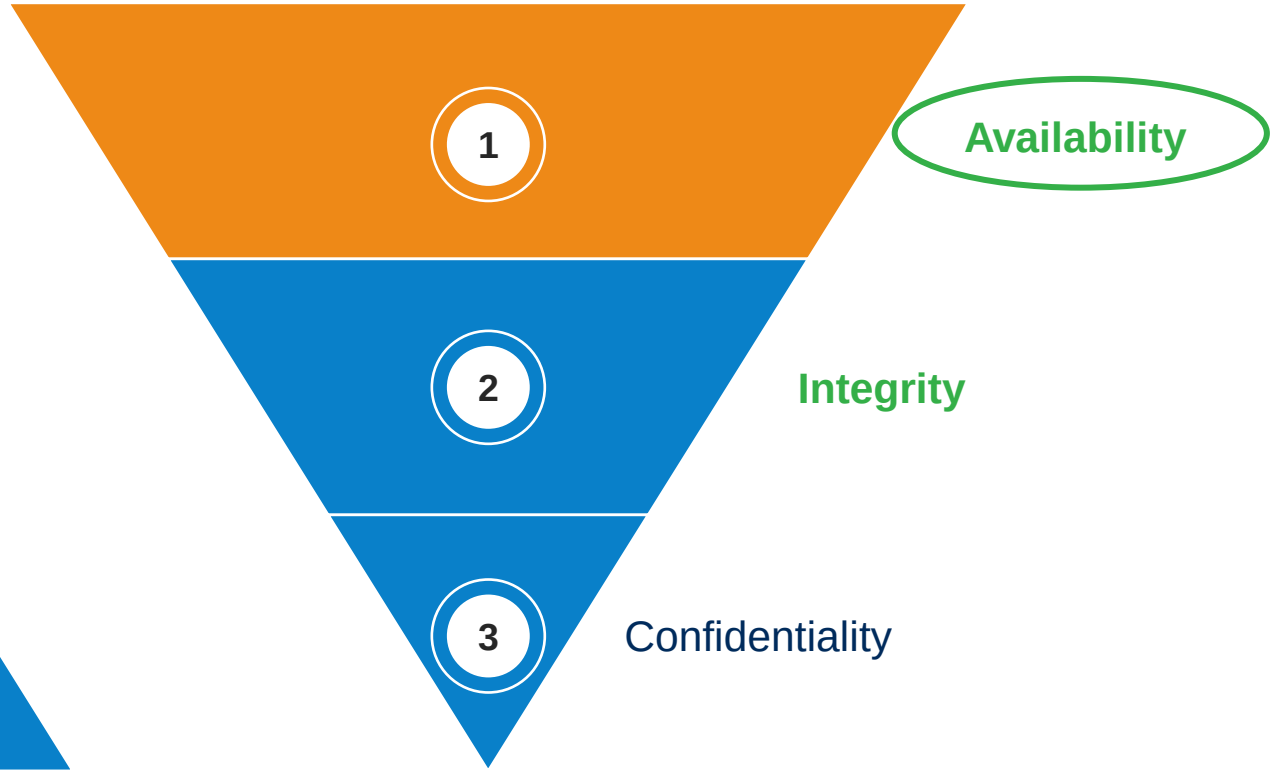
Getting in Sync - IT Cyber Priorities ≠ OT Cyber Priorities

Privacy-Driven



Information Technology

Safety & Continuity



OT or "Control Systems"

Risks are different for OT than IT systems. They must be treated different.

OT Cybersecurity

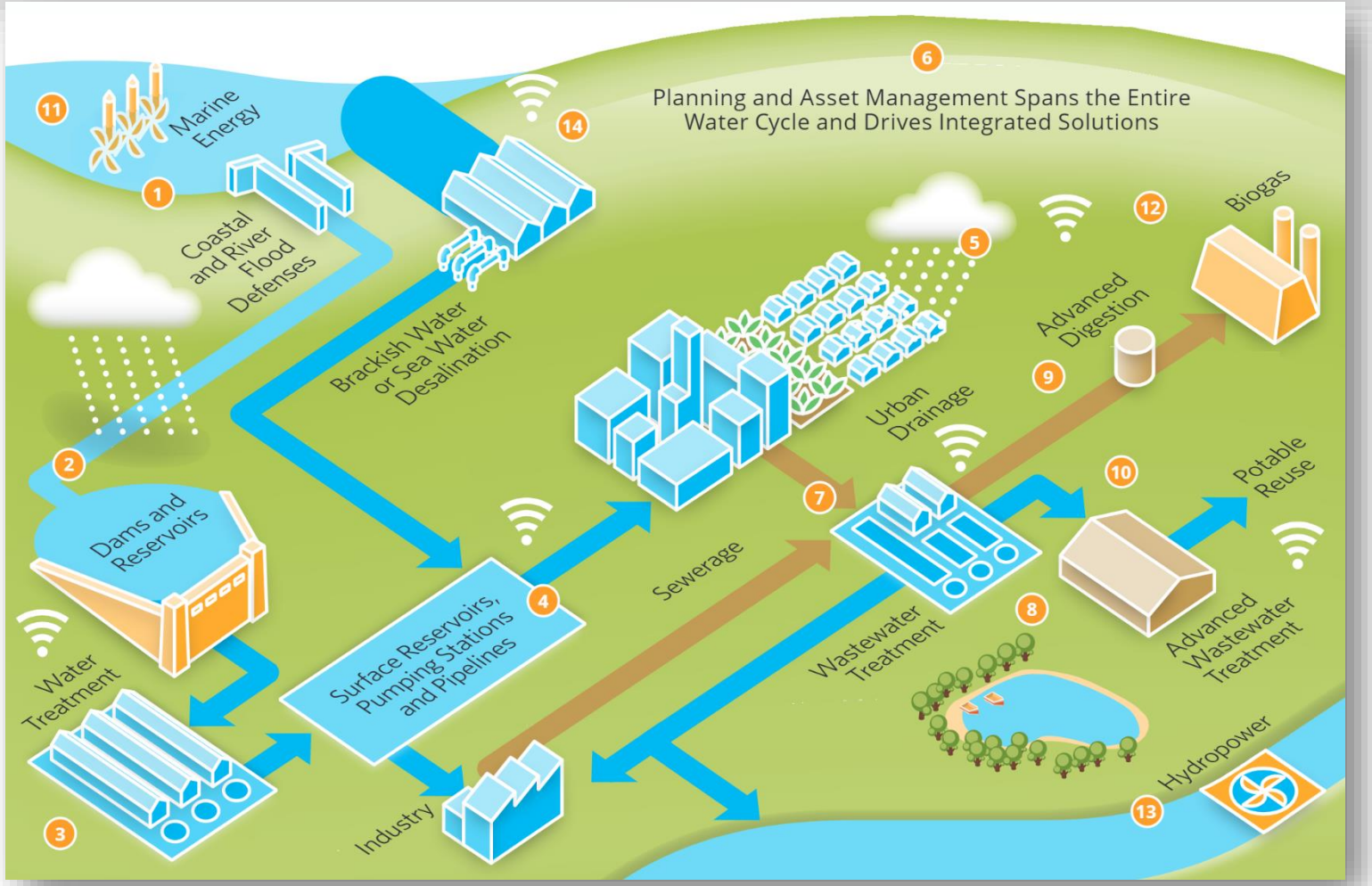
Why is it important?

- **Life Safety |** Unauthorized access could lead to overdosing chemicals, boil water alerts, insufficient water for fire-fighting.
- **Environmental Protection** | Unauthorized access could lead to under treatment, chemical release, and permit violations.
- **Business Continuity |** Unauthorized access could lead to permanent damage to equipment, extended manual operation, and "starting over" with control systems.
- **Effects of Automation |** Automation limits manual operation experience. Automation leads to downsizing and limits the number of staff that can respond. Utilities need automation to work.
- **Regulations** | Federal mandates likely . . . some states (e.g., FL, TN) prohibit ransomware payment.
- **Accountability** | Utility management must exercise due diligence and due care.

*"Cybersecurity is the art of **protecting** networks, devices, and data from **unauthorized access** or criminal use and the practice of ensuring **confidentiality, integrity,** and **availability** of information "*

– Cybersecurity & Infrastructure Security Agency (CISA)

Q: Which control systems are affected by cyber?



1. Climate Change Resilience
2. Dams & Reservoirs
3. Water Treatment
4. Conveyance & Storage
5. Stormwater & Flooding
6. Planning & Asset Management
7. Wastewater Collection & Treatment
8. Water Resources/Environmental
9. Biosolids Management
10. Water Reuse
11. Marine Energy
12. Cogeneration/Combined Heat & Power
13. Hydropower
14. Desalination

A: Control system cybersecurity can affect every part of a utility's core business.

2 Current State of Cybersecurity

U.S. Water and Wastewater System Cyber Attacks

Year	Ransomware Attacks	Remote Access - Based Attacks	Total	Cost
2018	2		**2**	$2.6M
2019	3	1	**4**	$1.5M, $18M
2020	5		**5**	$500K
2021	6	4	**10**	
2022	?	?	**?**	

Observations

- **Ransomware & Remote Access**
- **Expensive!**
- **Two 100% increases.**
- **Less detail in 2021?**
- **What happened in 2022?**
- **Problem solved?**

Ransomware and Remote Access are two areas that deserve special attention.

Ransomware Statistics from 2021

An ounce of prevention is worth a pound of cure . . . Think Pareto Principle (a.k.a. “80/20 rule”).

$2M average ransomware payment in energy, oil/gas and utilities

average cost to remediate an attack **$1.4M**

61% data recovered after payment

recovered ALL data after payment **4%**

Cybersecurity Regulations

Federal (passed)

- **America's Water Infrastructure Act (AWIA) of 2018**
- Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) of 2022
- **EPA Mandate – Water-Cyber part of state sanitary surveys – March 3, 2023**

Federal (future)

- Additional critical infrastructure cybersecurity requirements – chemicals, healthcare, etc.

State (Passed)

- **FL – Chapter 2022-220 (HB7055) – Adopt cyber standards consistent with best practices. Prohibits paying ransomware.**
- MD – HB1205 – Public/private water/sewer to assess vulnerabilities and develop a cybersecurity plan.
- NC – N.C.G.S. § 143-800(a) – Prohibits paying **ransomware**.
- NJ – SB647 – Develop cyber program, policies, plans, processes, and procedures to identify and mitigate cyber risks.
- TN – TN SB 2282 – Prepare and implement a cyber plan.

State (Pending)

- AZ – HB2145 – Prohibits paying **ransomware**.
- HI – HB2052 – Prohibits paying **ransomware**.
- PA – SB726 – Prohibits paying **ransomware**.
- NY – S6806A § 401 – Prohibits paying **ransomware**.
- TX – HB3743 – Prohibits paying **ransomware**.

If paying ransomware is illegal, what "extra" is being done to prevent an attack?

Florida Cyber Legislation

FL – Chapter 2022-220 (HB7055) – **Adopt cybersecurity standards** consistent with best practices. Prohibits paying ransomware (282.3186).

Section 3. Section 282.3185, Florida Statutes, is created to read:

282.3185 Local government cybersecurity.—

(1) SHORT TITLE.—This section may be cited as the "Local Government Cybersecurity Act."

(2) DEFINITION.—As used in this section, the term "local government" means any county or municipality.

(3) CYBERSECURITY TRAINING.— See

(4) CYBERSECURITY STANDARDS.—

*(a) Each **local government** shall **adopt** **cybersecurity standards** that safeguard its data, **information technology**, and information technology resources to ensure availability, confidentiality, and integrity. The cybersecurity **standards must be consistent with generally accepted best practices for cybersecurity, including the NIST Cybersecurity Framework ["CSF"]***.*

*(b) Each **county** with a **population of 75,000** or more must adopt the cybersecurity standards required by this subsection by **January 1, 2024**. Each county with a **population of less than 75,000** must adopt the cybersecurity standards required by this subsection by **January 1, 2025**.*

*(c) Each **municipality** with a **population of 25,000** or more must adopt the cybersecurity standards required by this subsection by **January 1, 2024**. Each municipality with a **population of less than 25,000** must adopt the cybersecurity standards required by this subsection by **January 1, 2025**.*

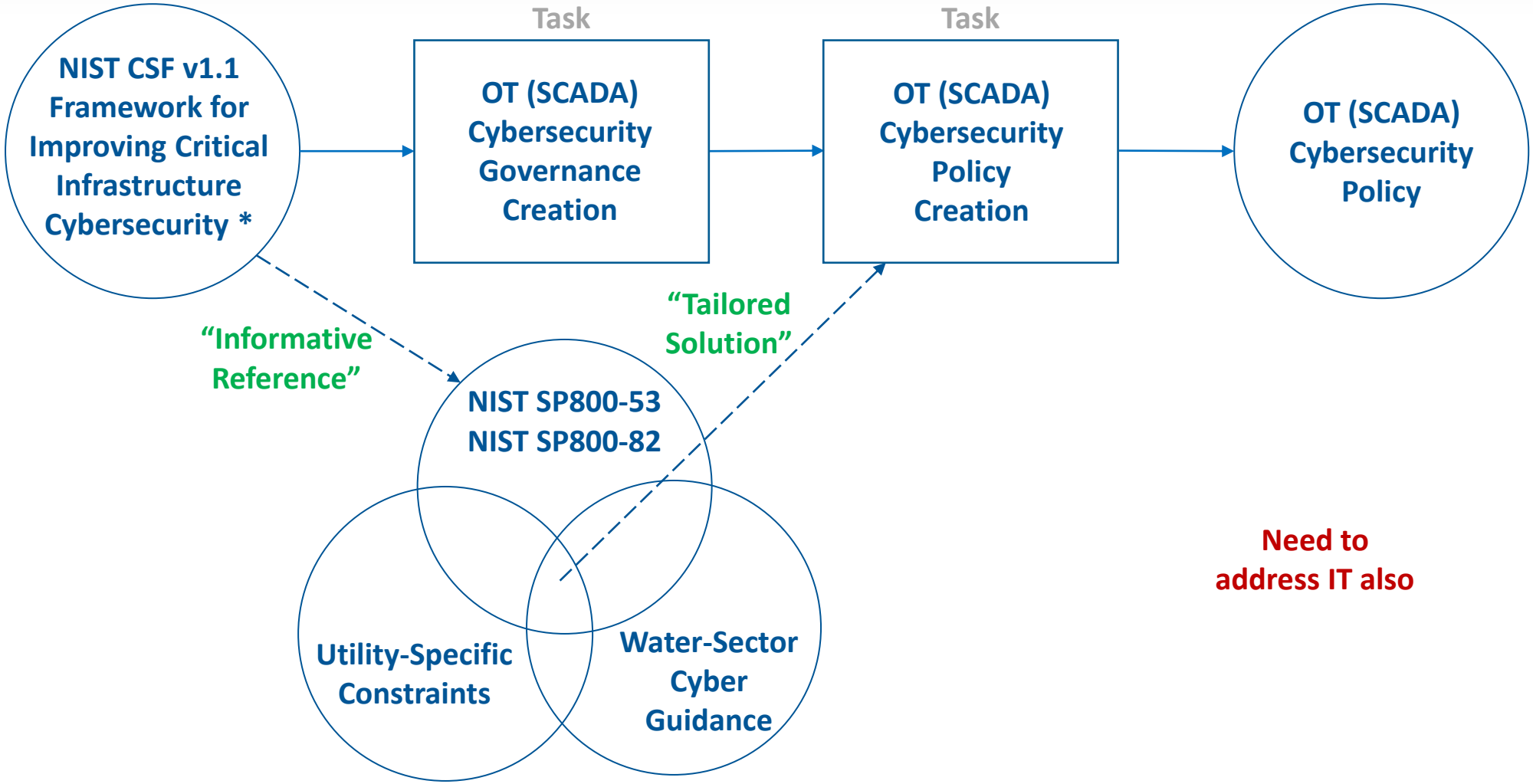
*(d) Each local government shall **notify the Florida Digital Service** of its compliance with this subsection as soon as possible.*

(5) INCIDENT NOTIFICATION.—

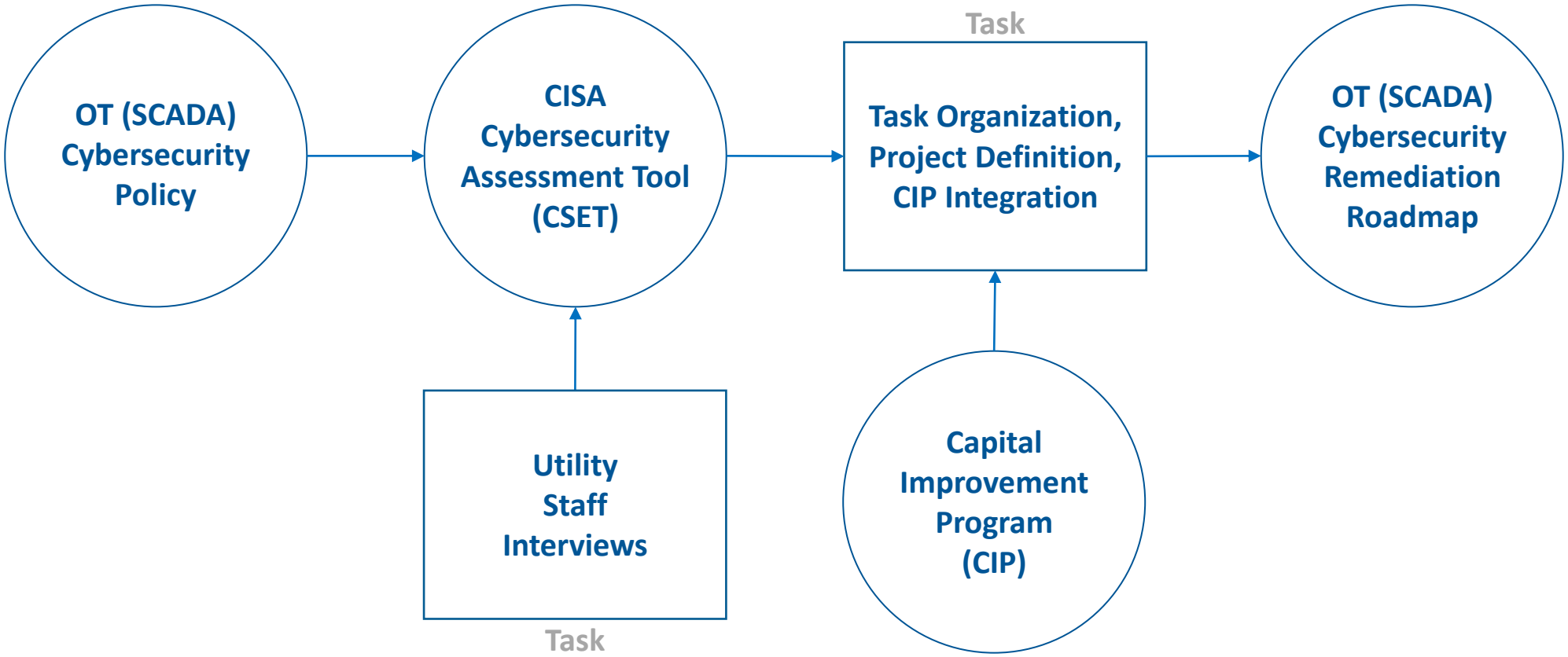
(6) AFTER-ACTION REPORT.—

"NIST Framework for Improving Critical Infrastructure Cybersecurity" = "Cybersecurity Framework" = "CSF"

NIST “Cybersecurity Framework” (CSF) Process



NIST “Cybersecurity Framework” (CSF) Process



EPA Water-Cyber Mandate

On March 3, 2023, the US EPA issued a memorandum to State Drinking Water Administrators which states:

- "states must **evaluate the cybersecurity of operational technology** used by a public water system [PWS] when conducting PWS **sanitary surveys** or through other state programs."
- "the goal of sanitary surveys is to ensure that states effectively **identify significant deficiencies** and that public water systems then **correct those significant deficiencies** - **including cybersecurity**-related significant deficiencies - that could impact safe drinking water."

EPA Water-Cyber Mandate

States have options for fulfilling their **assessment responsibilities** as part of sanitary surveys:

- Option 1a – PWSs may self-assess with a state-approved method (e.g., CISA Cyber Resilience Review - CRR, **NIST CSF**, **AWWA Cyber Tool**, ISO 27001, and ISA/IEC 62443). The EPA is also offering another option in the form of a checklist/tool; an Excel spreadsheet with the filename **Water Cybersecurity Assessment Tool and Risk Mitigation Plan Template.xlsx**. The recent release of **CISA's Cross-Sector Cybersecurity Performance Goals** were used to develop this checklist/tool.
- Option 1b – ". . . a PWS could undergo an **assessment** of cybersecurity practices **by an outside party**, EPA's Water Sector Cybersecurity Evaluation Program, or another government or private sector technical assistance provider approved by the state." The state must maintain a list of approved agents that can perform the assessments.
- Option 2 – States have the option of **using their surveyors** to evaluate the cybersecurity of PWSs themselves as part of the sanitary survey on-site inspections.
- Option 3 – States may use a **cybersecurity program they already** have or develop a new program that is "at least as stringent" as the new sanitary survey approach and repeated/updated just as often.

States have some important decisions to make.

EPA Water-Cyber Mandate

Observations:

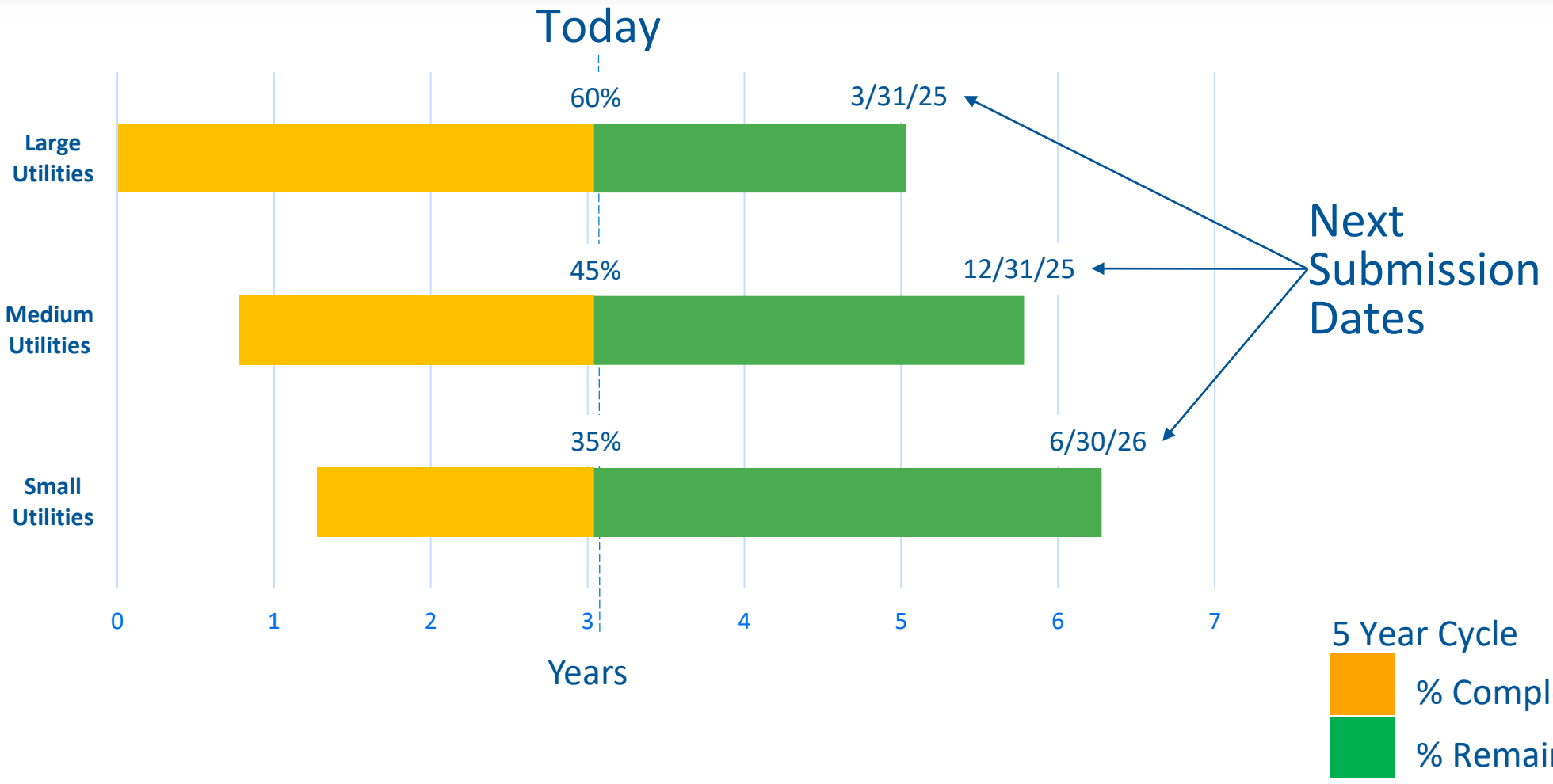
- There will be a **time delay** as states decide their specific approach.
- PWSs can proceed with confidence **after states decide** requirements.
- States must establish **what "significant cyber deficiency" means** to them.
- Deficiencies deemed **not "significant"** may end up **voluntary** for the PWS.
- **No deadlines or penalties** found for the states/PWS's to comply.
- EPA will make **changes** based on feedback received.
- The EPA wants PWSs to start assessing as soon as possible and not wait.

AWIA – America's Water Infrastructure Act

- Community water systems serving more than 3,300 people to develop or update Risk Assessments and Emergency Response Plans (ERPs).
- Includes cybersecurity assessments for IT and OT.

Population Served	Risk and Resilience Assessment	Next 5-Year Cycle Submission Date
≥ 100,000	March 31, 2020	March 31, 2025
50,000 - 99,999	December 31, 2020	December 31, 2025
3,301 - 49,999	June 30, 2021	June 30, 2026

AWIA – America's Water Infrastructure Act

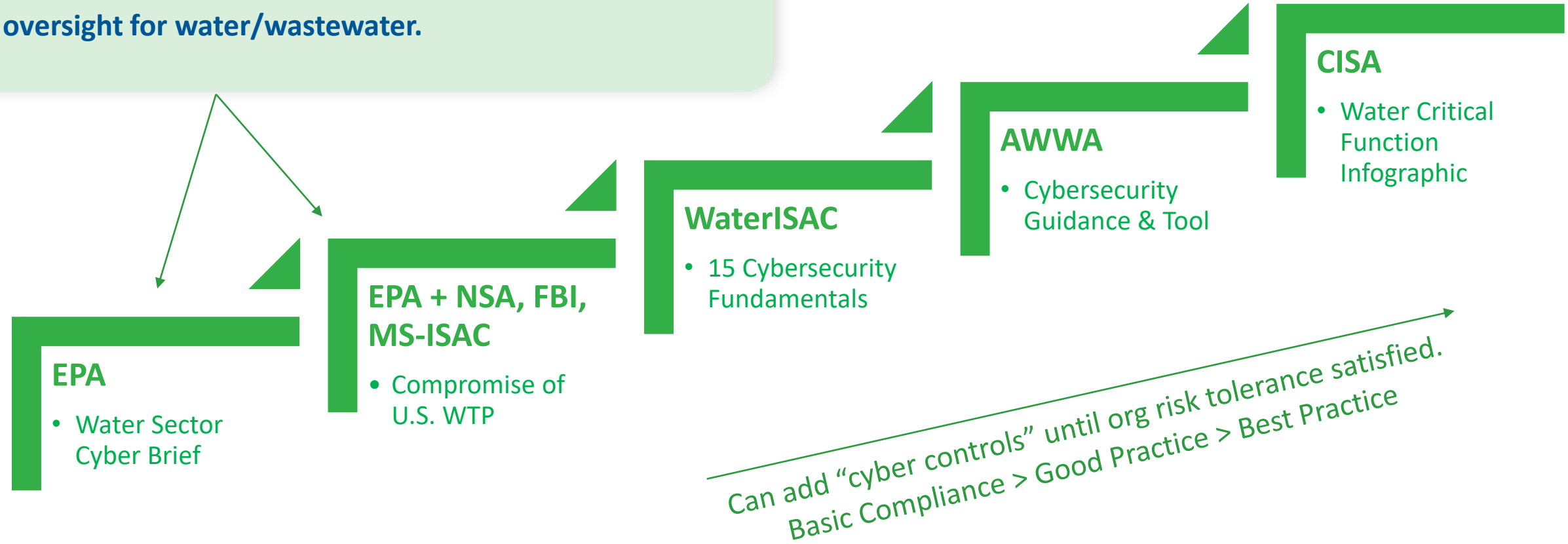


Are you on track to meet your goals?

3 Getting Started

Abundance of Water Sector Cybersecurity Guidance

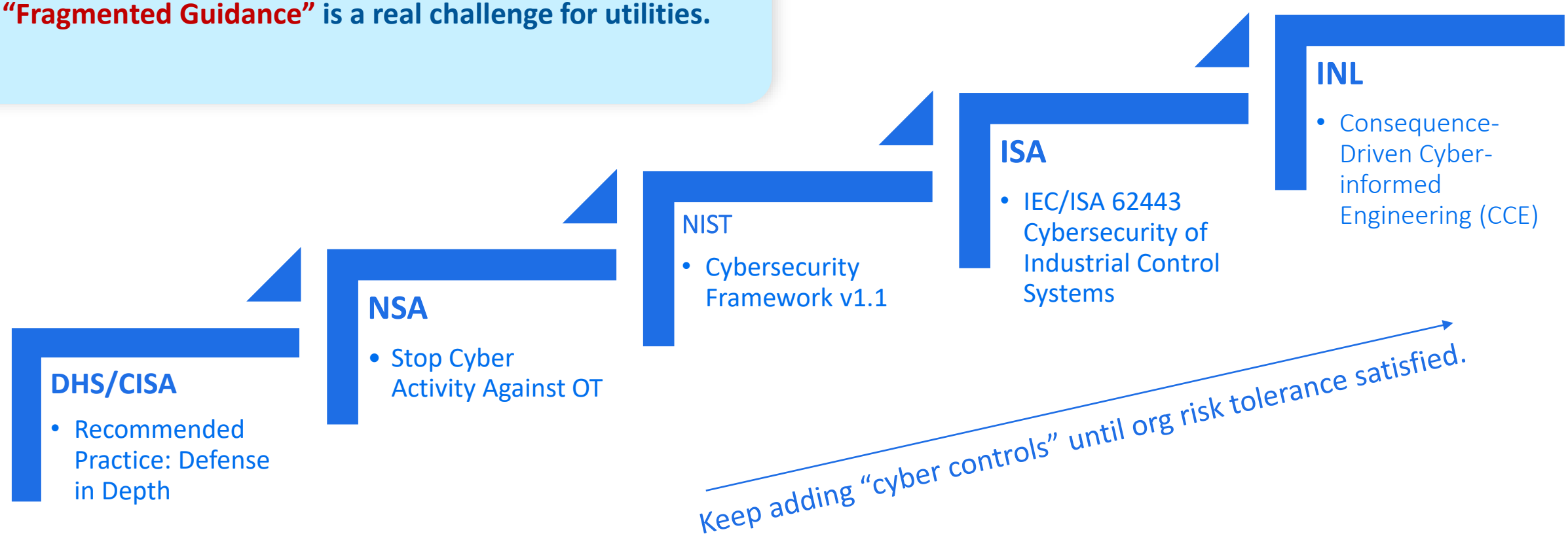
Start with EPA Guidance – They have cybersecurity oversight for water/wastewater.



If you were hacked, how would you explain not implementing this guidance?

Abundance of Generic Cybersecurity Guidance

"Fragmented Guidance" is a real challenge for utilities.



Too much guidance** prevents a **clear vision** and **actionable plan.

Cybersecurity of Critical Infrastructure

PLAN | IMPLEMENT | OPERATE

Identify

- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management
- Supply Chain

Protect

- Identity Management and Access Control
- Awareness Training
- Data Security
- Information Protection Processes and Procedures
- Maintenance
- Protective Technology

Detect

- Anomalies and Events
- Security Continuous Monitoring
- Detection Processes

Respond

- Response Planning
- Communications
- Analysis
- Mitigation
- Improvements

Recover

- Recovery Planning
- Improvements
- Communications

Proactive steps in each CSF category are needed for a holistic approach.

Cybersecurity Recurring Cyber Themes

- OT-DMZ
- Purdue Model
- Defense-in-depth
- Continuous Monitoring
- Remote Access
- Least Privilege

- Anti-virus
- Anti-malware
- Backups
- Training
- Asset Inventory
- Risk Assessment

Where do you stand? How do you know?

Cybersecurity Recurring Cyber Themes

- **OT-DMZ**
- **Purdue Model**
- **Defense-in-depth**
- **Continuous Monitoring**
- **Remote Access**
- **Least Privilege**

- Anti-virus
- Anti-malware
- Backups
- Training
- Asset Inventory
- Risk Assessment

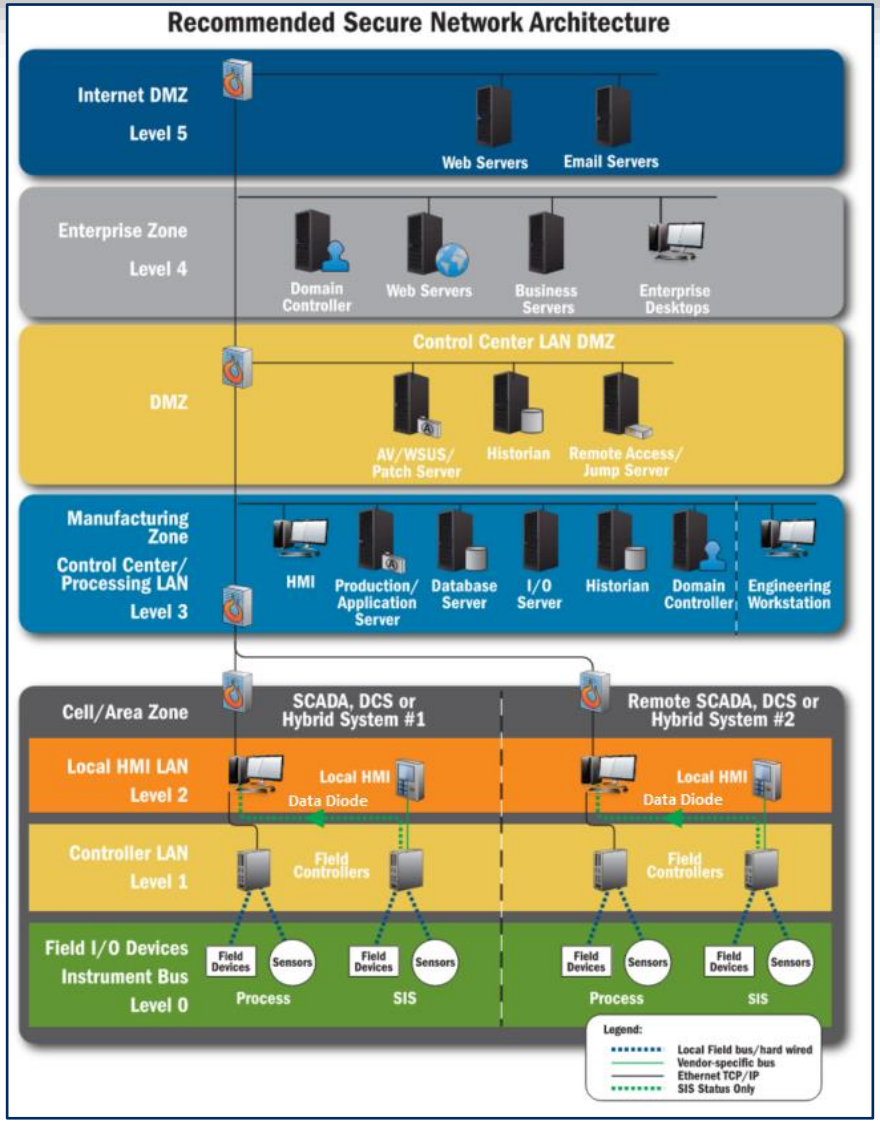
Where do you stand? How do you know?

Network Segmentation / DMZ

- DHS version of the Purdue Model
- No direct IT/OT communication
- All traffic terminates in OT-DMZ
- Increase “work effort” of adversary
- OT-DMZ: remote access jump server, patch server, Tier-2 historian, read-only web portal, file server, email relay, syslog server, etc.
- Defense-in-depth

IT

OT



Source: DHS - Improving Industrial Control System Cybersecurity with Defense-in-Depth

Cybersecurity Recurring Cyber Themes

- OT-DMZ
- Purdue Model
- Defense-in-depth
- Continuous Monitoring
- Remote Access
- Least Privilege

- **Anti-virus**
- **Anti-malware**
- **Backups**
- Training
- Asset Inventory
- Risk Assessment

Where do you stand? How do you know?

Cybersecurity Recurring Cyber Themes

- Anti-Virus
- Anti-Malware
- Updates & Patching
  - Operating Systems
  - Applications – HMI, Office, programming software
  - Firmware for PLCs and instrumentation
- Backups
  - Periodic testing

Updates, Patching, & backups are the main defender against Ransomware

Cybersecurity Recurring Cyber Themes

- OT-DMZ
- Purdue Model
- Defense-in-depth
- Continuous Monitoring
- Remote Access
- Least Privilege

- Anti-virus
- Anti-malware
- Backups
- Training
- Asset Inventory
- Risk Assessment

Where do you stand? How do you know?

Our Philosophy

Consider adopting this philosophy yourself.

BLACK & VEATCH

Cybersecurity Is Risk Management:

- We know OT risk should not be treated the same as IT risk.
- We know it is best to follow industry guidance and not reinvent the wheel.
- We know that one size does not fit all.
- We know that a work plan with too many controls in too short of a time period will likely fail.
- We know people need a common vision to achieve a challenging goal.
- We know it is easier to change course incrementally than all at once.

Contact Information

Jim Schultz

SchultzJ@BV.com
913-458-6970

Laurie Kusmaul

KusmaulLM@BV.com
754-229-3081

Questions?

Jim Schultz
SchultzJ@BV.com
913-458-6970 (Eastern)