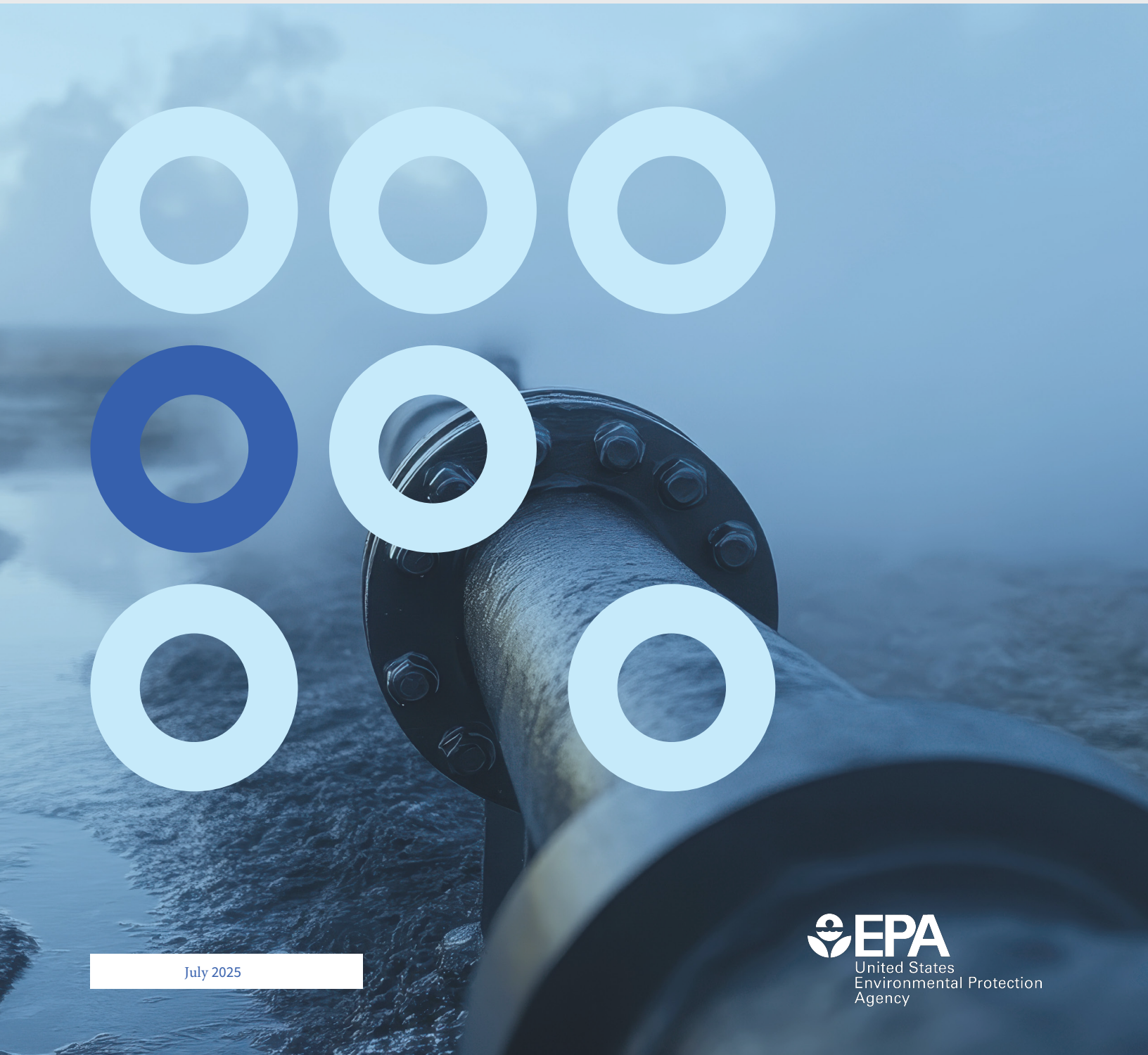
SECURING THE FUTURE OF WATER:

Addressing Cyber Threats Today



July 2025

EPA
United States
Environmental Protection
Agency

SECURING THE FUTURE OF WATER: ADDRESSING CYBER THREATS TODAY

Drinking water and wastewater systems are essential to public health, safety, and economic vitality. These systems, while robust, are vulnerable to cyber threats. Cyber-attacks on the water sector pose significant risks, including the potential to disrupt operations, compromise water quality, and cause substantial economic losses.[1]

For over a decade, EPA and its water sector partners—including federal agencies, national associations, state entities, and utilities—have collaborated to strengthen the sector's cybersecurity posture. In 2024, EPA convened and served as the co-chair of a Water Sector Cybersecurity Task Force (Task Force), under the auspices of the Water Sector Coordinating Council (WSCC) and Government Coordinating Council (GCC), to identify and prioritize recommendations for improving cybersecurity in the water sector. As co-chair, EPA facilitated the development of the recommendations which represent a continuation of previous efforts, with a renewed focus on collaboration and alignment to amplify impact and build resilience across the sector.

Navigating Cybersecurity Challenges in Today's Water Utilities

Water utilities rely heavily on both Information Technology (IT) and Operational Technology (OT). IT systems manage enterprise functions (e.g., email, billing), and OT systems control physical operations (e.g., water treatment). Many of these systems were designed before today's heightened cyber risk environment, and their integration has introduced vulnerabilities that can be difficult to address.

Compounding these challenges:

1. Aging OT systems are incompatible with modern IT security protocols.
2. Upgrades require significant capital and operational planning, which is often out of reach for lower-capacity utilities.
3. Other imperatives can out compete cybersecurity for attention with legitimate alternative priorities (e.g., regulatory requirements) taking precedence.

CRITICAL INFRASTRUCTURE DEPENDENCE

Water utilities are the backbone of public health and economic stability, ensuring safe drinking water, sanitation, and uninterrupted operations for communities and businesses.

[1] Office of the Director of National Intelligence. (2024, June). Recent cyber attacks on *U.S. infrastructure underscore vulnerability of critical U.S. systems*. Retrieved from Recent Cyber Attacks on US Infrastructure Underscore Vulnerability of Critical US Systems, November 2023–April 2024

Not all utilities look the same. Drinking water and wastewater utilities face distinct policy, regulatory, and operational contexts that influence their incentives and decision-making around cybersecurity. To effectively reach all utilities, efforts must acknowledge and adapt to these differences.

Target Audience for the Task Force Recommendations

The Task Force identified two distinct types of utilities that are a priority focus for short-term actions to advance cybersecurity practice.

- **Lower-capacity utilities** that struggle with limited resources, making it difficult to implement even basic cybersecurity measures.
- **Higher-capacity utilities** that have resources but may not prioritize cybersecurity due to competing demands like aging infrastructure.

Additionally, the Task Force recognized utility executive leadership as a critical audience. By engaging top decision-makers, who set priorities and allocate resources, the Task Force aims to ensure cybersecurity receives the necessary attention to drive meaningful and sustained improvements sector-wide.

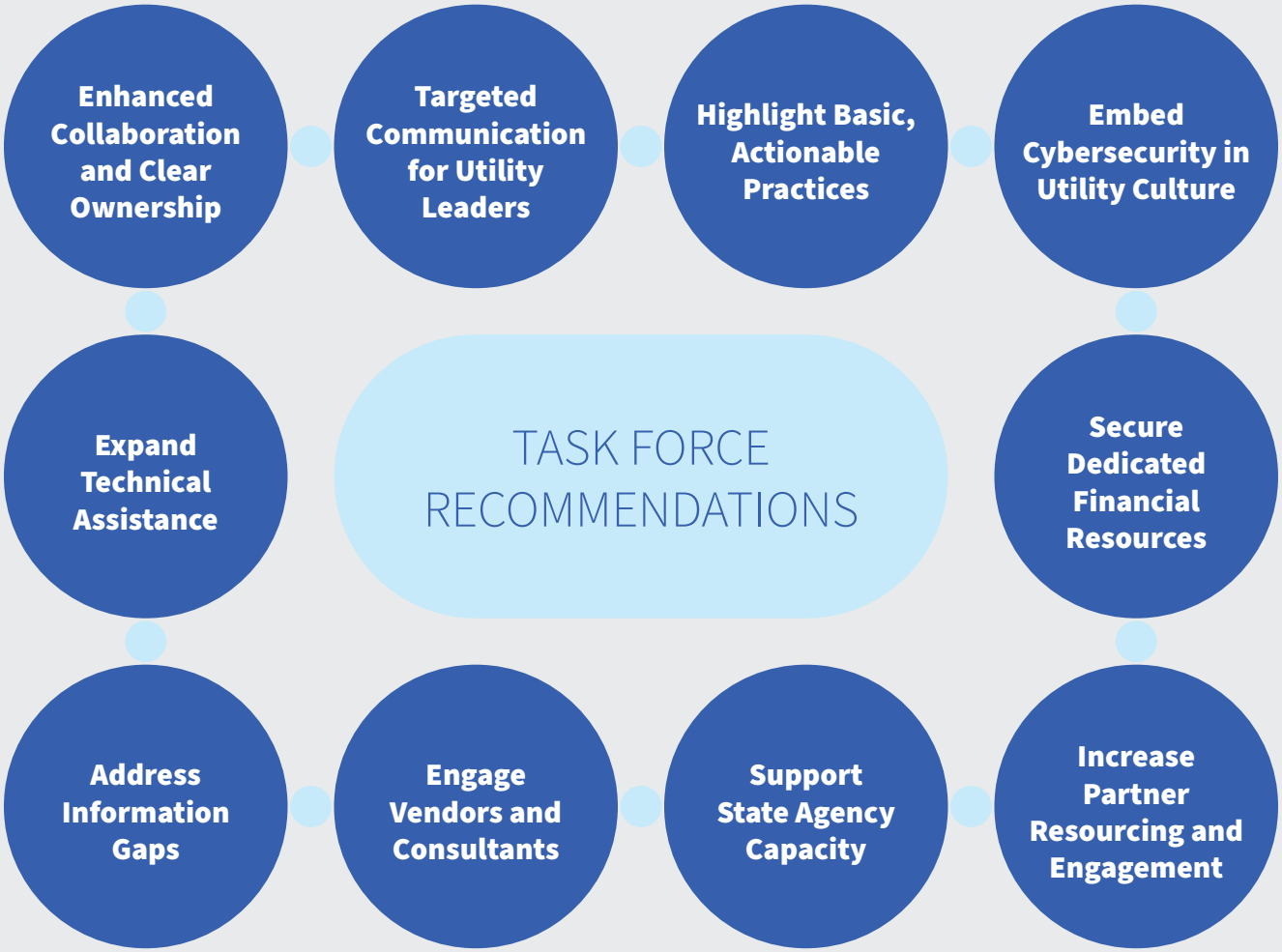
The Task Force Recommendations: A Unified Framework for Action

The 10 recommendations of the Task Force are designed to work together as an integrated framework to strengthen the cybersecurity posture of the water sector. Each recommendation addresses a specific challenge while complementing the others to create a comprehensive, coordinated approach. Key aspects of how the recommendations function together include:

- **Building Momentum Through Collaboration:** Enhancing partnerships across federal agencies, states, utilities, and national associations ensures alignment, coordination, and shared responsibility.
- **Targeting Executive Leadership:** Recognizing the critical role of utility executive leadership, the Task Force emphasizes tailored communication strategies and leadership training to "break through" competing priorities.
- **Tailored Support for Diverse Utilities:** Addressing the unique needs of both lower-capacity and higher-capacity utilities ensures that all water systems can take meaningful steps toward improving cybersecurity.
- **Focusing on Foundational Practices:** Highlighting key, actionable steps provides utilities with clear priorities, reducing complexity and enabling progress even with limited resources.
- **Expanding Resources and Expertise:** Increasing access to technical assistance, training, and financial resources empowers utilities to overcome barriers to cybersecurity implementation.
- **Embedding Cybersecurity into the Sector's Culture:** Sustained efforts to promote cybersecurity practices help normalize and prioritize these measures across the sector.

SUMMARY OF THE RECOMMENDATIONS AND PRIORITY ACTIONS

The Task Force developed the following recommendations, which the WSCC and GCC adopted. Each recommendation lists actions in priority order. Together, these recommendations create a unified strategy to drive immediate and lasting improvements in the water sector's cybersecurity resilience. Their implementation will require commitment and cooperation from all stakeholders, ensuring progress toward a safer and more secure future for critical water infrastructure.



1

Enhanced Collaboration and Clear Ownership

Enhance Water Sector collaboration and establish clear ownership of recommendations to support proactive coordination, alignment, and responsibility for advancing these cybersecurity recommendations.

PRIORITY ACTIONS

1. **Define Clear Ownership and Responsibility**
2. **Align Expectations and Resource Planning**
3. **Establish a Standing, Collaborative Forum**

2

Targeted Communication for Utility Leaders

Develop and launch a targeted communication strategy specifically designed for drinking water and wastewater utility executive leadership to effectively reach utilities and increase uptake of cybersecurity practice.

PRIORITY ACTIONS

1. **Develop a Targeted Communication Strategy for Drinking Water and Wastewater Utility Leadership**
2. **Develop a Water-Sector Focused Cybersecurity Leadership Training**
3. **Expand Engagement to Broader Executive Leadership**
4. **Integrate Cybersecurity into Leadership Training Programs**

3

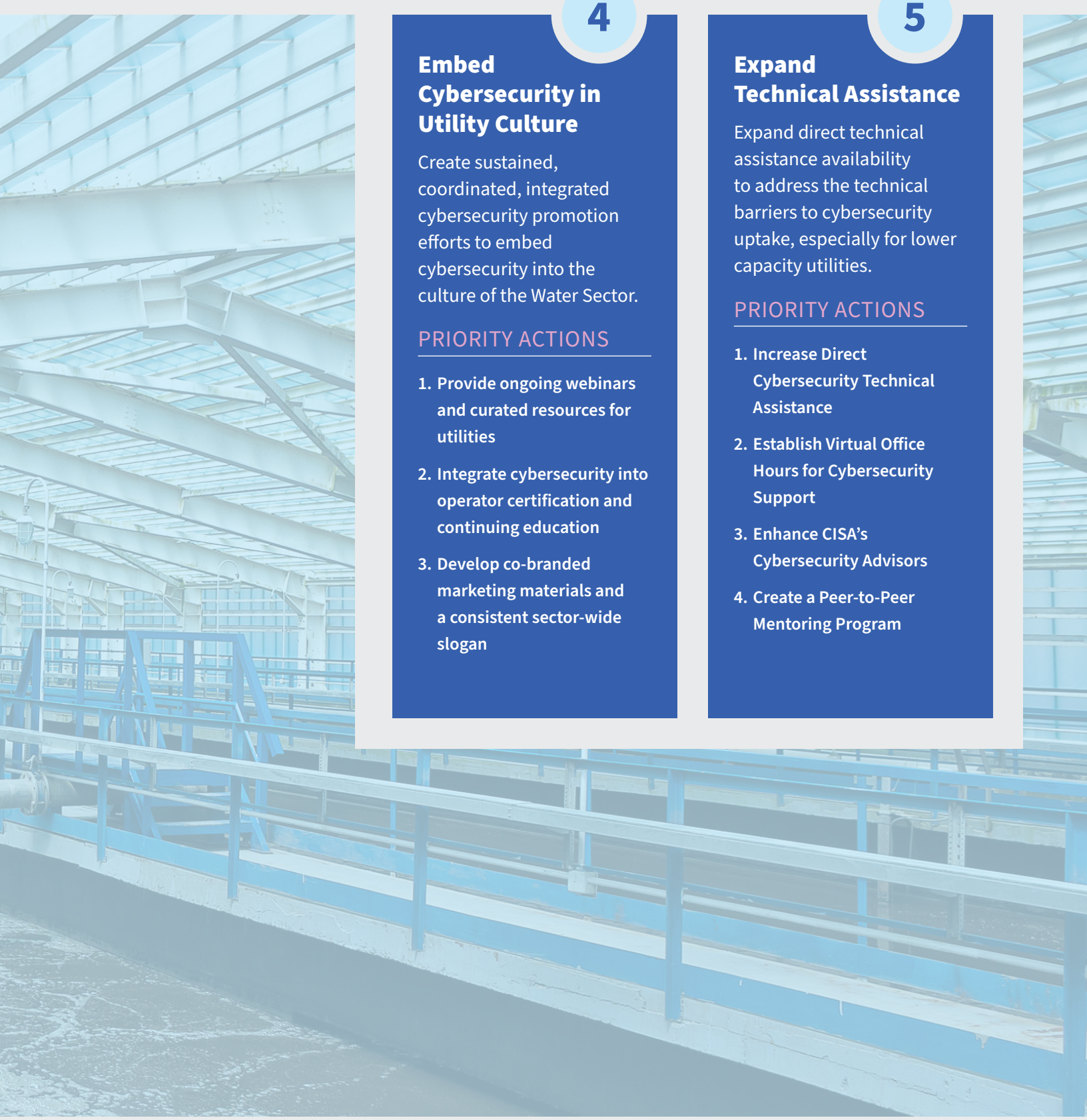
Highlight Basic, Actionable Practices

Highlight a limited number of important and attainable basic cybersecurity practices that all utilities should adopt for their protection and to lay the foundation for a sustainable cybersecurity program and culture.

PRIORITY ACTION

Assemble a common set of basic cybersecurity practices to anchor joint, promotional efforts drawing on the following elements:

- **Lead with Commitment**
- **Equip with Training**
- **Assess Utility External Exposure and Understand IT/OT Assets**
- **Block Unauthorized Access**
- **Create Incident Response Plan**



4

Embed Cybersecurity in Utility Culture

Create sustained, coordinated, integrated cybersecurity promotion efforts to embed cybersecurity into the culture of the Water Sector.

PRIORITY ACTIONS

1. **Provide ongoing webinars and curated resources for utilities**
2. **Integrate cybersecurity into operator certification and continuing education**
3. **Develop co-branded marketing materials and a consistent sector-wide slogan**

5

Expand Technical Assistance

Expand direct technical assistance availability to address the technical barriers to cybersecurity uptake, especially for lower capacity utilities.

PRIORITY ACTIONS

1. **Increase Direct Cybersecurity Technical Assistance**
2. **Establish Virtual Office Hours for Cybersecurity Support**
3. **Enhance CISA's Cybersecurity Advisors**
4. **Create a Peer-to-Peer Mentoring Program**

6

Secure Dedicated Financial Resources

Secure dedicated, directed financial resources to ensure utilities and states are appropriately and adequately resourced to advance cybersecurity practices.

PRIORITY ACTIONS

1. **Include Cybersecurity in Executive Agency Budget Requests**
2. **Increase WaterISAC Funding for Free Utility Access**
3. **Modify Federal Grant and Loan Program Eligibility**
4. **Coordinate with State Chief Information Officers (CIO) Offices for Cybersecurity Support**
5. **Fund State-Level Risk and Resiliency Coordinators**

7

Address Information Gaps

Address gaps in current cybersecurity information resources and make it easier for utilities to find and access existing tools and knowledge needed to improve their cybersecurity posture.

PRIORITY ACTIONS

1. **Create a Summary of Recent Cyber Attacks and Breaches**
2. **Create a Central Clearinghouse for Best Practices**
3. **Bolster Collaboration**
4. **Identify and Promote Model Policies and Practices**
5. **Develop a Compendium of Cybersecurity Implementation Examples**

8

Engage Vendors and Consultants

Engage and educate IT/OT consultants, consulting engineers, and industrial controls and other vendors on consequences and the needs of utility operators to assist in building resilience, support manual operations, and secure by design.

PRIORITY ACTIONS

1. **Provide Model Service Contracts and Key Questions**
2. **Develop Cybersecurity Principles for Vendors**
3. **Increase Vendor Awareness of Cybersecurity Risks**
4. **Clarify Cybersecurity Expectations in Service Agreements**
5. **Recruit Vendor Participation**

9

Support State Agency Capacity

Support the increased capacity of state primacy agencies (SDWA), authorized agencies (CWA), other existing relevant state entities, and Water Sector partners to leverage their well-developed, trusted relationships to support utility education and training and to increase information sharing.

PRIORITY ACTIONS

1. **Engage States as An Active Partner in Delivering Short-Term Cybersecurity Messaging**
2. **Deliver In-Person Cybersecurity Training**
3. **Document and Share State Cybersecurity Program Practices**
4. **Equip Field Engineers and Training Staff with Cybersecurity Messaging**

10

Increase Partner Resourcing and Engagement

Increase cyber resourcing and engagement by existing and new partners at the state and local level (e.g., Technical Assistance Providers, SLTTs) to leverage trusted organizations and relationships to provide technical assistance, deliver consistent messaging, coordinate action, and increase reach to advance adoption of cybersecurity practices in the Water Sector.

PRIORITY ACTIONS

1. **Leverage Trusted Partners to Deliver Essential Training and Technical Assistance**
2. **Engage Major SLTT Membership Organizations**
3. **Scale Up Trusted Partners to Deliver Cyber Support**
4. **Leverage and Promote Water Sector Cybersecurity Workforce Development**

FROM RECOMMENDATIONS TO ACTION: WHAT'S NEXT?

Implementing these recommendations will be crucial to supporting the water sector and its vital role in safeguarding public health, safety, and the economic vitality of our communities.