BURNS McDONNELL

WHITE PAPER / **RISK AND RESILIENCY COMPLIANCE**

THE TICKING CLOCK FOR AWIA COMPLIANCE ON RISK ASSESSMENT AND EMERGENCY RESPONSE PLANS

BY Victor Elazegui, CPP, PSP, AND **Jason Vigh,** CISSP

America's Water Infrastructure Act (AWIA) sets into motion a timeline for risk and resiliency compliance requirements for community water systems. A cohesive, comprehensive approach that incorporates best practices for infrastructure resiliency, physical security and cybersecurity can keep you ahead of fast-approaching compliance deadlines.

What makes water infrastructure essential is also what makes it a target: Clean, reliable water is vital for both human health and economic stability. As the threat environment in the United States continues to evolve, increased concerns about water security have bubbled to the surface.

WHAT AWIA CHANGES

With the signing of the AWIA into law in October 2018, community water systems (CWS) now have defined requirements — and approaching deadlines — for risk assessments and emergency response. Drinking water utilities serving more than 3,300 people must complete risk and resiliency assessment (RRA) and emergency response plan (ERP) certification requirements, including a review of physical security and cybersecurity measures.

The legislation also transitions from a terrorism or intentional act vulnerability assessment approach to an "all-hazards" risk and resiliency assessment approach. This encompasses not just malevolent acts but also natural or accidental hazards. The EPA recently released a Baseline Information on Malevolent Acts for Community Water Systems document, which identifies specific threat categories and establishes a starting point for the consideration of threat likelihood.

The EPA states these preparations are intended to help water utilities "identify, deter, detect and prepare for these threats; reduce vulnerabilities of critical assets; and mitigate the potential consequences of incidents that do occur." Approached with gravity and strategy, the development process is a valuable tool, broadening an organization's perspective and increasing its capabilities to respond to any risk.

Completing the assessment and emergency response plan, while necessary, may feel like an enormous challenge to a water utility already operating on a limited budget. But the cost of noncompliance is expensive, with fines of up to $25,000 per day when RRAs and ERPs are not certified by their respective deadlines. Even greater is the potential tangible and intangible costs of lack of preparation if a malevolent incident should occur.

POPULATION SERVED	RISK ASSESSMENT	EMERGENCY RESPONSE PLAN
100,000+	Due March 31, 2020	Sept. 30, 2020
50,000-99,999	Due Dec. 31, 2020	June 30, 2021
3,301-49,999	Due June 30, 2021	Dec. 30, 2021

FIGURE 1: *Emergency response plan certifications are due six months from the date of the risk assessment certification. The dates shown above are certification dates based on a utility submitting a risk assessment on the final due date.*

Larger CWS may have regulatory-focused staff to handle the considerable compliance efforts. But medium- and small-sized utilities may struggle to manage the process. The American Water Works Association (AWWA) suggests supplementing internal resources with third-party support. Consultants — especially those with experience in water system infrastructure, other utility infrastructure, physical security and cybersecurity — can help guide utilities through each step.

KNOWING YOUR INFRASTRUCTURE AND RISKS

The EPA doesn't establish a specific methodology for completing the RRA, so it's up to a utility and its resource partner to determine the most efficient and effective process while complying with AWIA requirements. Before a utility can accurately assess risk, it must determine what's critical to it as an organization from an infrastructure, physical security and cybersecurity standpoint. Only when a system is known can it be accurately protected.

While the final component is an ERP, the work begins with gaining a detailed understanding of a CWS' infrastructure. While some utilities have robust asset management plans and a thorough list of assets, some may have inherited a partial list or no asset list at all. Often, this information is stored inside an employee's head rather than a digitized, GIS-based system — and with employee turnover, the knowledge base decreases.

A CWS should consider the worst-case scenario as a plausible occurrence, because in today's threat environment, it is. What are the hazards that can take water services offline and impact the ability to serve customers? For example, most utilities have a single source supply, which brings a host of associated risks. Is a secondary source available? Is an emergency connection contract to another utility in place? Exploring these vulnerabilities and considering solutions form the foundation of the ERP.

BEST PRACTICES FOR PHYSICAL SECURITY

The measures behind maintaining a physically secure environment are rarely convenient. Just getting into a facility may require unlocking a gate, keeping track of an access badge, scanning in without tailgating in behind someone and signing in an access log. Employees may find themselves irritated, or even resistant, to such measures.

Employees are often the most effective security measure in an organization. Since the ability to effectively deter or mitigate a threat is only as strong as its weakest link, employees can also be a significant vulnerability. Something as innocent as leaving a door unlocked or allowing a suspicious activity to go unreported can pose a danger.

CONSIDER THESE BEST PRACTICES WHEN SUPPORTING THE PHYSICAL SECURITY COMPONENT OF AWIA COMPLIANCE:

- **Obtain executive leader sponsorship.**
- **Create, distribute and provide timely training on security-related changes that impact the general employee population, including security systems, policies and procedures.**
- **Create and distribute security-related reminders, such as posters, pamphlets, email communications and presentations.**

Identifying an effective method of influencing security best practices while maintaining regulatory compliance is a common challenge security practitioners encounter. Totally eliminating the vulnerability of human error is impossible. However, increasing employee security awareness and leveraging employees to support and enhance security detection and deterrence capabilities turns a vulnerability into part of the solution.

BEST PRACTICES FOR CYBERSECURITY

AWIA represents the first instance of cybersecurity consideration in risk assessments and emergency plans for the water industry. Given that almost every water utility incorporates some level of network capability, it's a timely and relevant inclusion. Risks associated with cyberattacks have steadily increased. And even if the system doesn't allow an attacker to physically open or close a valve, for instance, that individual could trick a sensor to display normal monitoring levels while a malevolent actor physically tampers with it.

As with a utility's physical assets, a good understanding of an organization's OT assets is a first step. Since compliance requirements haven't addressed this before, it's a new area of measurement. With networks and data management systems continuing to grow so quickly, working toward a full understanding of how OT systems interact with infrastructure and physical security systems can be an eye-opening exercise.

Even if a CWS has cybersecurity professionals on staff, those employees may not have the bandwidth to add these compliance responsibilities to their everyday workload. These best practices — many already in place in other utility markets — can help inform AWIA compliance process:

- Segment your networks until the right cybersecurity elements are in place. While there's often a push from a workload perspective to converge operational networks with IT infrastructure, this opens up considerable vulnerability. Air gapped networks can be compromised.

- Sometimes updates aren't performed to avoid taking down the network and impacting service. Keep systems up to date with available patches.
- When incorporating new technology, establish training programs and processes so employees can use the tools effectively. Then test and measure frequently.
- Incorporate devices that provide visibility into IT infrastructure so operators can understand the traffic patterns, increasing their ability to identify malevolent forces.

PRIORITIZING TO BUILD RESILIENCY

If you lose a pump on your intake structure or power to your pump station, can you keep running? If your chemical tank is ruptured and you lose supply of a specific coagulant, can you get more or keep treating water another way? The risk assessment identifies a utility's most critical vulnerabilities and helps rank them for action.

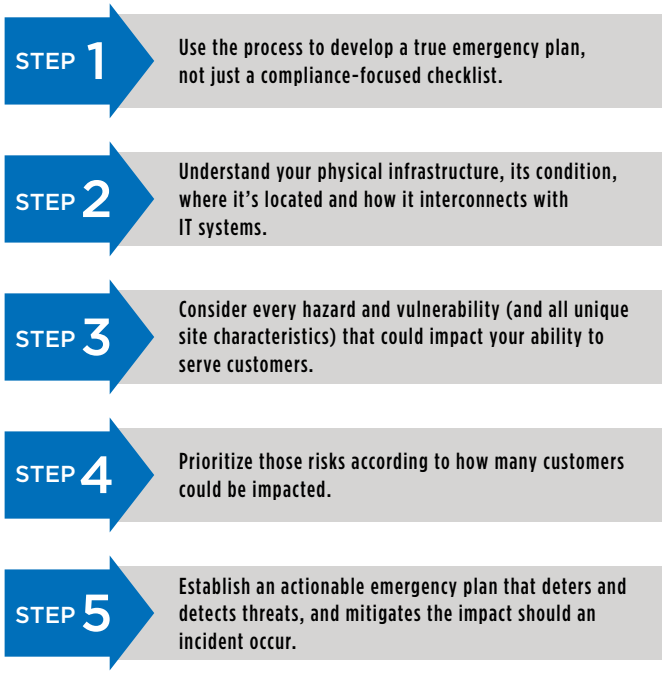

FIGURE 2: *Steps for establishing water system resiliency.*

The ERP is that action plan. While it's based on the results of the assessment, it also includes several other elements, including planning partnerships with other utility departments, coordination with local law enforcement and public health officials, and a public relations and communications strategy for emergency situations.

It's helpful to walk through the scenarios and responses related to potential incident types, from a tornado or act of terrorism to a simple loss of power. The probability of the scenario helps determine the priority of the risk — and the budget that should be allocated to minimizing its chances.

ACHIEVING EFFECTIVE THREAT MANAGEMENT

The introduction of AWIA will help a CWS better prepare for the possibility of malevolent and natural-based threats, enhancing its ability to respond to incidents and improving the reliability of delivering clean water. Compliance-driven regulations, although certainly a necessity and in this particular case critical to unhindered drinking water operations, can overwhelm organizations without the available resources to achieve them.

The steps associated with conducting an RRA and updating an ERP offer a great opportunity for a utility to establish or build upon existing water system resiliency and physical and cybersecurity programs. Incorporating subject matter leaders and specialists within the AWIA process can help ease the effort. As physical and cyberthreats become increasingly prevalent and sophisticated, critical infrastructure utilities are recognizing the importance of developing (or maturing toward) a dedicated threat management team. Achieving AWIA compliance efforts — in a strategic and timely manner — can represent a significant step forward.

BIOGRAPHIES

VICTOR ELAZEGUI, CPP, PSP, is a project manager at Burns & McDonnell. His work centers on maturing physical security programs, aligning program objectives with organization missions and goals, and the identification of effective threat and vulnerability mitigation solutions. Victor has completed the AWWA Utility Risk and Resilience Certificate Program.

JASON VIGH, CISSP, is a cybersecurity manager at 1898 & Co. His background includes work for a wide range of industries, including financial services, information technology consulting and aviation. Jason has completed the AWWA Utility Risk and Resilience Certificate Program.

ABOUT BURNS & McDONNELL

Burns & McDonnell is a family of companies bringing together an unmatched team of engineers, construction professionals, architects, planners, technologists and scientists to design and build our critical infrastructure. With an integrated construction and design mindset, we offer full-service capabilities with more than 60 offices globally. Founded in 1898, Burns & McDonnell is 100% employee-owned. For more information, visit **burnsmcd.com**.

ABOUT 1898 & CO.

1898 & Co. is a business, technology and cybersecurity consulting firm serving the industries that keep our world in motion. As part of Burns & McDonnell, our consultants leverage global experience in critical infrastructure assets to innovate practical solutions grounded in your operational realities. For more information, visit **1898andCo.com**.

15562-RRC-0621