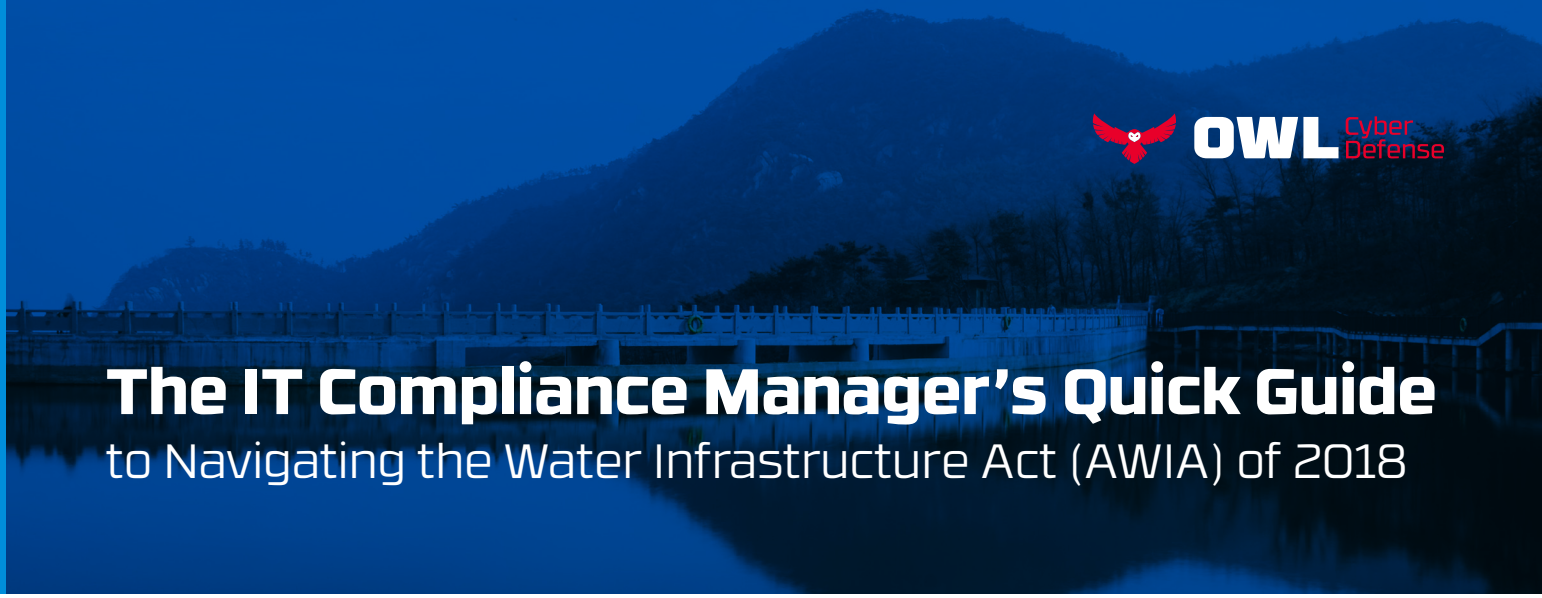
DATA SHEET



The IT Compliance Manager's Quick Guide
to Navigating the Water Infrastructure Act (AWIA) of 2018

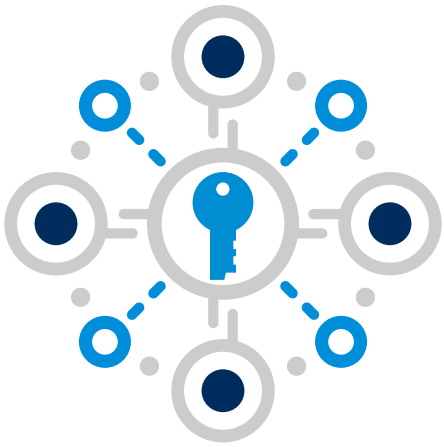
Your one-stop resource to help you navigate cybersecurity compliance for water utilities....

So you've heard about America's Water Infrastructure Act (AWIA) of 2018, that was released in October. But do you know the what, why, and how it effects your organization? What does your team need to take action on?

Say no more – we've sifted through the (lengthy) document to bring you the most important AWIA cybersecurity compliance facts and figures. Rest assured this cheat sheet will have you on your way to being AWIA cybersecurity compliant (and score you some bonus points with the boss).

What is the AWIA?

- AWIA stands for America's Water Infrastructure Act
- Signed into law in October 2018 by President Donald Trump
- One of the most monumental water infrastructure packages passed by Congress
- Designed to grow economy, keep communities safer, reduce bureaucratic "red tape"
- Supports and creates sustainable paying jobs in the U.S.
- Incentivizes businesses to buy and use American products



Why Does It Matter?

- Invests $6 billion for improvements to America's critical water and wastewater infrastructure
- Deauthorizes $4 billion in water resources development projects that Congress deems are no longer viable, relevant, or feasible
- Targets repairs and upgrades to drinking water systems, dams, reservoirs, levees, and ports
- Requires that water utilities conduct risk and resilience assessments
- Authorizes and expands clean drinking water initiatives for the first time in two decades

What do I need to do to comply?

Submit a letter of certification to the U.S. Environmental Protection Agency stating the utility has performed risk & resilience assessment and created an emergency response plan based on the staggered schedule according to population served:

POPULATION	RISK & RESILIENCE ASSESSMENT DEADLINE	EMERGENCY RESPONSE PLAN
100,000+	3/31/2020	9/30/2020
50,000 - 99,999	12/31/2020	5/30/2021
3,300 - 49,999	5/30/2021	12/30/2021

Compliance Action Plan: Defense in Depth

When developing your compliance action plan, consider that layers of security are required to defend against modern cyberattacks. This layered approach is referred to as “defense-in-depth” and is featured in many cybersecurity best practices and regulatory guidance documents, such as the U.S. Department of Homeland Security’s “Seven Steps to Effectively Defend Industrial Control Systems.”

Owl’s data-diode based products are used by many critical infrastructure operators today as an integral part of a defense-in-depth security architecture. To learn more about how Owl data diode cybersecurity can help protect water and wastewater systems, check out our whitepaper – “OPDS Supports DHS Seven Strategies.”

OWL Cyber Defense

Owl Cyber Defense Solutions, LLC leads the world in data diode and cross domain network cybersecurity. With a constant focus on customers in the military, government, critical infrastructure, and commercial communities, Owl develops market-first, one-way data transfer products to meet a variety of operational needs, from entry level to enterprise.

For more information on Owl, or to schedule a demo, visit www.owlcyberdefense.com

@OwlCyberDefense

203-894-9342 | Info@owlcyberdefense.com