



Complying with America's Water Infrastructure Act of 2018 (AWIA)



Section 2013 of AWIA

Section 2013 of the America's Water Infrastructure Act of 2018 (AWIA) requires community water systems serving over 3,300 people to complete a risk and resilience assessment and develop an emergency response plan. The deadlines for submitting a certification of completion to the Environmental Protection Agency (EPA) depend on the population served by the drinking water utility.



Population Served

- $\geq 100,000$
- 50,000-99,999
- 3,301-49,999

Risk Assessment

- March 31, 2020
- December 31, 2020
- June 30, 2021

Emergency Response Plan

- September 30, 2020
- June 30, 2021
- December 30, 2021

How Forescout SilentDefense Helps Water Utilities Comply with AWIA

Risk Assessment

Automatically create an inventory of all network assets and a network baseline.

SilentDefense provides the control system role for each device on the network/s, along with providing the model number, firmware version, serial number, and common vulnerabilities and exposures (CVEs) for each.

Optimize cyber and operational risk assessment processes by focusing on business impact risks using the **Asset Risk Framework – which identifies and scores both cyber and operational risks for individual hosts**. All of this information is easily exportable in various formats for easy compliance documentation.

The Industrial Threat Library (ITL) features 2,400+ ICS-specific threat indicators. These indicators include security, networking and operational data, providing a **holistic view of risks and the ability to correlate events** across all three of these domains.

Continuous OT network security monitoring technology **detects security and operational events using a medley of hybrid techniques** based on custom threat profiling, anomaly detection, queries and rules-based analysis.

How Forescout SilentDefense Helps Water Utilities Comply with AWIA

Emergency Response Plans

SilentDefense alerts provide **rich contextual information about the source, nature and target of a threat**, along with key input for its analysis (including packet capture related to the threat) to enable a quick response.

Dedicated tools and an API empower responders to **quickly search the network for advanced threat indicators**. All of this data is formatted for consumption by other systems, including asset repositories, SIEMs, compliance reporting systems, correlation engines, and others.

Network and protocol baselines generated by SilentDefense can be used in recovery situations to **automate remediation actions** and help **ensure devices and applications are operating as expected**.

Visual network analytics allow incident responders to **perform forensic analysis on both real-time and historical network activity**.

Ready to Start Your Risk and Resilience Assessment for AWIA?

Request a Demo



Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Int'l) +1-408-213-3191
Support +1-708-237-6591

Learn more at [Forescout.com](https://forescout.com)

© 2019 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at www.forescout.com/company/legal/intellectual-property-patents-trademarks. Other brands, products, or service names may be trademarks or service marks of their respective owners.