# Xage Security enables compliance for America's Water Infrastructure Act of 2018

Over the last few years the scale and severity of cybersecurity attacks have increased significantly against U.S. infrastructure. In addition, processes are more automated, digitized and interconnected than ever in order to improve efficiency, and as a result, many municipalities and water utilities are more susceptible to these escalating attacks. The impact of a successful cyber-attack, specifically in the water sector, pose risks not only to the infrastructure but also the surrounding environment and service area population.

In 2018 Congress passed the America's Water Infrastructure Act (AWIA) of 2018 that requires utilities to conduct risk assessments for water systems and certify to the Environmental Protection Agency their completion. This risk assessment includes addressing measures to ensure system resilience of automated systems which includes cybersecurity considerations. In response to this mandate, the American Water Works Association's Cybersecurity Guidance and Assessment Tool was created to assist utilities in aligning with best practices and regulations such as the NIST Cybersecurity Framework and Section 2013 of America's Water Infrastructure Act of 2018. Collectively these resources provide the water sector with a voluntary, sector-specific approach for implementing applicable cybersecurity controls and recommendation. The most significant recommendation for protection is the use of identity-based access control for industrial devices and software in order to protect these control systems even if the operational network is breached.

Xage delivers industrial-grade security in a single application to defend, prevent, and identify malevolent cyber-attacks against any industrial component in your industrial water operations. Operators are empowered to manage user and device identities, credentials, and access control policies with ease and without networking-based IT skill sets. The Xage Security application is designed to run within your industrial environment supporting both legacy and modern devices and applications regardless of vendor or network type in order to avoid the need to replace assets currently installed.

The Xage Security Application exceeds NIST Framework for Cybersecurity and W-ISAC Cybersecurity Fundamentals guidelines. This paper details how Xage's application can address the risks outlined specifically in these guidelines and American Water Works Association's Cybersecurity Guidance and Assessment Tool.

# Xage Security Suite Map for AIWA Detailed Category Mapping

*Requirements nomenclature from AWWA Cybersecurity Guidance and Assessment Tool

| REQMT* | Description | Priority | Category | Details | Xage Value |
|---|---|---|---|---|---|
| **AU-1** | Audit program established to ensure information systems are compliant with policies and standards and to minimize disruption of operations. | 1 | Application Security | IT schedules an independent review and examination of records and activities to assess the adequacy of system controls and to ensure compliance with established policies. | Xage captures and provides tamper-proof audit logs that contain detailed information about user/device access activity. Thus enabling and facilitating audits to ensure all access was approved by the organization policy |
| **IA-1** | Access control policies and procedures established including unique user ID for every user, appropriate passwords, privilege accounts, authentication, and management oversight. | 1 | Access Control | Based on their knowledge of access control policies, operators do not share passwords. | Xage platform manages user, device (legacy and new) and application identities and access policies. Xage access policy defines interactions and operations an identity can perform. Xage offers flexibility to enable fine-grained control on the authentication process to comply with security standards, such as configuring password complexity, password expiration, password/key rotation and multi-factor authentication. Managing all the devices and identities with Xage reduces operational cost (easier to manage access across the entire enterprise and operation which may contain many different devices, applications, and users), provides better management oversight (visibility into user access log, and who has access to what in a single location), enforces authentication which conforms with compliance and eliminates the need for shared accounts. |
| **IA-10** | Policies and procedures for least privilege established to ensure that users only gain access to the authorized services. | 1 | Governance and Risk Management | If no user is logged in at a SCADA screen, a read-only view is presented. Individual roles created and assigned to users depending on their responsibilities. | Xage provides Role-Based access and control capabilities which allows not only to determine which users have access to which device/application/data, but also what actions can that user perform on that device/application/data (e.g read/write etc..) |
| **IA-11** | Workstation and other equipment authentication framework established to secure sensitive access from certain high risk locations. | 1 | Access Control | Access to control of critical equipment is only available at a secured terminal. | Xage provides flexible access control capabilities. When securing a sensitive device, it is possible to allow access to that device only from a certain machine. Furthermore, it is possible to configure access based on the specific users from that machine. It is even possible to allow a group of machines access to that device (not only a single machine). |
| **IA-2** | Access control for the management, monitoring, review, and audit of accounts established including access control, account roles, privilege accounts, password policies and executive oversight. | 4 | Access Control | Upon staff termination or resignation, login credentials are disabled as part of the Human Resources process. | Xage manages all identities and access policies in a central location - a single policy is required to revoke the terminated user access rights. This policy change can also be automated using the Xage REST API and integrated into existing workflows. In addition, Xage provides tamperproof audit logs which can facilitate auditing of user access and access policy. |
| **IA-3** | Role based access control system established including policies and procedures. | 1 | Access Control | SCADA software implements unique usernames and passwords with different levels of control based on roles. | See IA-10 |

| REQMT* | Description | Priority | Category | Details | Xage Value |
|---|---|---|---|---|---|
| **IA-4** | Access control for confidential system documentation established to prevent unauthorized access of trade secrets, program source code, documentation, and passwords (including approved policies and procedures). | 1 | Access Control | Defined clearance requirements for individuals to access confidential information. | Xage can protect sensitive digital data, by only allowing access to authorized users/devices/applications on per data segment and topic level. |
| **IA-5** | Access control for diagnostic tools and resources and configuration ports. | 1 | Access Control | PLC programming software is only available at select workstations and only accessible to SCADA technicians. | See IA-11 |
| **IA-6** | Access control for networks shared with other parties in accordance with contracts, SLAs and internal policies. | 1 | Access Control | Contracts with third-party equipment vendors establish security requirements for remote access to equipment. | Xage role-based access control can be used to facilitate LAN sharing across multiple parties securely - ensuring each party only has access to resources they are allowed to access and also enabling parties to share data securely, with strict access control and tamperproofing. |
| **IA-9** | Multifactor authentication system established for critical areas. | 1 | Access Control | Remote access to the SCADA system requires two factor-authentication. | Xage enables implementing unified MFA across the entire fleet, including legacy and new devices and applications, even when those devices have no security controls implemented. |
| **PE-2** | Secure areas protected by entry controls and procedures to ensure that only authorized personnel have access. | 1 | Access Control | Access to the server room is restricted to authorized staff only. | Xage manages identities and access policy. Xage can integrate with any existing enforcement system (such as a badging system). Using a single system to manage all the identities and access policies make it easy to operate and consistently maintain security posture, enforcing standard policies and reducing operating cost. |
| **SC-1** | Policies and procedures governing cryptography and cryptographic protocols including key/certificate-management established to maximize protection of systems and information. | 1 | Governance and Risk Management | When selecting new PLCs for a system upgrade, SCADA techs evaluate the option of using newer PLCs that offer encryption for communication. | Xage secures communication between devices such as PLCs and RTUs. Securing communication is done automatically and dynamically by defined access policies that allow devices to communicate. Xage unique capabilities can secure communications between devices that lack encryption and access control capabilities, making it possible to adhere to compliance requirements without having the need to replace existing equipment. |
| **SC-12** | Remote access framework including policies and procedures established to provide secure access to telecommuting staff, established for the management, monitoring, review, and audit of remote access to the organization. | 1 | Access Control | Remote access to the SCADA system requires two factor-authentication. | See IA-9 |

| REQMT* | Description | Priority | Category | Details | Xage Value |
|---|---|---|---|---|---|
| **SC-2** | Centralized authentication system or single sign-on established to authorize access from a central system. | 1 | Access Control | Operators have one username and password for PCS equipment which is managed from a central system. | Xage serves as a single authentication and authorization point to the entire system, providing single sign-on across the organization, making it possible to use a single username and password to access all the equipment the identity is allowed to access. Xage identities are managed centrally, but enforcement is done at the edge (i.e on-site) and does not rely on network communication to the center. |
| **SC-24** | Communications links encrypted. | 1 | Encryption | All data transferred via the wired network is encrypted using current wired communication best practices. | See SC-1 |
| **SC-7** | Information exchange protection program in place to protect data in-transit through any communication system including the Internet, email, and text messaging and approved policies and procedures. | 2 | Telecommunications, Network Security, and Architecture | Web applications for SCADA software use encryption to protect data in transit. | See SC-1 |
| **SC-8** | Routing controls established to provide logical separation of sensitive systems and enforce the organization's access control policy. | 2 | Telecommunications, Network Security, and Architecture | Within the SCADA system network, vendor systems are placed on a separate subnet rather than being on a single "flat" network. | With Xage, devices can be isolated or segmented regardless of the underlying network infrastructure (i.e even if the devices are on the same subnet, Xage will block network traffic between identities which are not allowed to communicate). The same concepts are true for users accessing devices - users will not have network connectivity until they have authenticated to Xage, and they have the proper authorization to do so. This does not only fulfill the requirement but also takes it one step further to achieve Zero-Trust. |
| **SI-3** | Interactive system for managing password implemented to ensure password strength. | 1 | Access Control | When configuring a new user's password, it must meet minimum character length requirements. | Xage enforces a flexible and configurable password policy across all devices and users it protects. Therefore it is easy to ensure passwords meet the desired password complexity (minimum length, specific characters, etc...) as well as enforcing password expiry, and denying password reuse. Xage makes this possible for legacy equipment that does not meet password complexity standards. |

## About Xage

The Xage Security Suite is the first and only blockchain-protected security platform for the Industrial Internet of Things (IIOT). Xage creates the essential trusted foundation for secure interactions between machines, people, and data. Advancing beyond traditional security models, Xage distributes authentication and private data across the network of devices, creating a tamper-proof "fabric" for communication, authentication and trust that ensures security at scale. Xage supports any-to-any communication, secures access to existing industrial systems, underpins continuous edge-computing operations even in the face of irregular connectivity, and gets stronger and stronger with every device added to the network. Xage customers include leaders in the largest industries, spanning energy, utilities, transportation and manufacturing.