Appendix - Definitions

Table of Contents

Access Control List – A written list of people authorized to access a system.

Account Privileges – The permissions assigned to an account that defines what systems they can access and change.

Administrative Functions – Functions not involved with water system operations. Examples include email, internet, meter reading, and billing.

Administrative Privileges – Permissions or privileges within a system to make major changes to a system. Administrative privileges provide greater ability to modify the system beyond those needed by an ordinary user to complete routine work.

Anticipated Corrective Action – Proposed actions to reduce the risk to a system by reducing or eliminating the vulnerability of an asset or system to a threat or by reducing or eliminating the consequence to the asset or system should a vulnerability be successfully exploited.

Application Allowlisting – Software which allows only approved programs or applications to be run on a computer system.

Authorized Personnel – Someone who has been granted access to a facility or system for the purpose of carrying out their duties.

Auto-scan of Removable Media – A process by which a computer scans removable media, such as USB drives, upon insertion. The auto-scan may execute malware before its presence on the media is detected.

America's Water Infrastructure Act of 2018 (AWIA) – Law enacted in 2018. Section 2013 of AWIA requires community water systems serving more than 3,300 people to develop or update risk and resilience assessments (RRA) and emergency response plans (ERP) and certify to U.S. EPA every five years the RRA and ERP have been created or updated.

Business Continuity Plan (BCP) – A plan which addresses the potential financial effects of a crisis, as well as the systems flexibility to adapt human resource policies to meet the changing needs of employees. Provides an overall indicator of a systems commitment to integrating risk management principles into the management culture that supports their operations.

Business Enterprise Systems – Informational technology (IT) systems used to carry out business functions such as email, meter reading, billing, and internet access. Business enterprise systems should be separate from the process control system (PCS).

Consequence –The adverse impacts that result when a threat occurs which damages or impairs the operation of the system's asset. It includes the economic costs, both to the system and the service area, due to equipment damage and loss of water service. Consequences also include injuries and fatalities that could result from accidental or intentional contamination of drinking water or a hazardous gas release.

Credentials – User login names, passwords, tokens, cards, or other information assigned to a person to access a system.

Critical Asset – A system component or asset which, if disabled or destroyed, would significantly impair the ability of a system to carry out its mission.

Cyber Security Audit – A systematic evaluation of how well a system conforms with established cybersecurity standards.

Cyber Security Event – Unauthorized access into a computer system, including a process control system or business enterprise system.

Data Backups – The creation of a second or back up copy of data that can be used if the primary data becomes inaccessible. Backed up data can include stored data, system settings, and other information needed to fully restore a system in the event of failure or compromise. Backups should be stored in a physically separate location to minimize the risk from loss due to physical destruction.

Data Transfer – Sending data or information from one place to another. Data can be transferred numerous ways, including using the internet, phone lines, radio frequencies, and direct hardwired lines.

Delay – Security measures intended to increase the amount of time it takes unauthorized people to reach an asset.

Detection – Security measures intended to detect when unauthorized people gain or attempts to gain unauthorized access to an asset.

Deterrence – Security measures intended to discourage or deter people from attempting to gain unauthorized access to an asset.

Dial Back Protocol – A communication protocol in which a computer or system, such as SCADA, seeking to connect with a remote device contact or calls the remote device using an assigned number. Upon receiving the initial contact, the remote device disconnects from the original number and then contacts the originating computer or system back on a different, predetermined number. The originating computer answers the call back and the needed information is exchanged.

Electronic, Computer, or other Automated Systems (including the security of such systems) – Encompasses all treatment and distribution process control systems, business enterprise information technology (IT) and communications systems (other than financial) and the processes used to secure such systems. Includes the sensors, controls, monitors, and other interfaces, plus related IT hardware and software and communications used to control water collection, treatment, and distribution. Also includes IT hardware, software, and communications used in business enterprise systems. The assessment must account for the security of these systems (e.g., cybersecurity and information security).

Emergency Response Plan (ERP) – A plan which contains immediate response actions for all types of incidents. Also includes contact and other important information which may be used while responding to an incident.

Encryption – The process of securing data by converting it from a readable format into an unreadable, or encrypted format. The encrypted data can only be made readable again by decoding it using the password or key.

Financial Infrastructure – Equipment and systems used to operate and manage utility finances. Possible examples include billing, payment, and accounting systems, along with third parties used for these services. This asset category is not intended to address the financial “health” of the water utility (e.g., credit rating and debt-to-equity ratios).

Firewall – A network security system that monitors and controls incoming and outgoing network traffic.

Incident Command System (ICS) – A standardized approach to the command, control, and coordination of on-scene incident management, providing a common hierarchy within which personnel from multiple organizations can be effective. ICS is the combination of procedures, personnel, facilities, equipment, and communications operating within a common organizational structure designed to aid in the management of on-scene resources during incidents. It is used for all kinds of incidents and is applicable to small and minor incidents, large and complex incidents, and planned events.

Information Security Officer – The person within an organization responsible for overseeing and protecting the organization’s network, data, and related infrastructure from threats.

Local Area Network – A computer network that interconnects computers within a limited geographic area, such as a building or facility.

Malevolent Act – A threat caused by an intentional act for the purpose of disrupting system operations.

Malicious Software (Malware) – Software designed to infect a computer or system with the intent of causing harm. Examples include viruses, worms, spyware, and ransomware.

Monitoring Practices –The processes and practices used to monitor source water and finished water quality, along with any monitoring systems not captured in other asset categories. Includes meters, sensors, laboratory resources, routine distribution monitoring, sampling capabilities, and data management equipment and systems.

> Note: Monitoring associated with physical security should be addressed under Physical Barriers, monitoring associated with process controls and cybersecurity should be addressed under electronic, computer, or other automated systems, monitoring associated with financial systems should be addressed under Financial Infrastructure.

Multifactor Authentication (MFA) – An access control method in which the user is only granted access to the system only after providing two or more different types of information confirming the user's identity.

Mutual Aid and Assistance – Agreements between other utilities and jurisdictions to provide resources in response to incidents. Establishes the details, such as liability and cost recovery, for providing resources beforehand so assistance can be provided as quickly as possible. Participation in such agreements is traditionally at no cost and does not obligate participants to respond.

National Incident Management System (NIMS) – Establishes a common framework for defining roles and responsibilities to enhance incident response. NIMS uses the Incident Command System (ICS) to provide the support structure for response activities.

Natural Hazard – Threat caused by acts of nature. Examples include hurricanes, flooding, and drought.

Operation and Maintenance of the Utility – Encompasses critical processes required for operation and maintenance of the water system that are not captured under other asset categories. Includes equipment, supplies, and key personnel. Assessments may focus on the risk to operations associated with dependency threats like loss of utilities (e.g., power outage), loss of suppliers (e.g., interruption in chemical delivery), and loss of key employees (e.g., disease outbreak or employee displacement).

Operations and Maintenance Manual (O&M) – A detailed document which contains the instructions and information needed to operate and maintain a piece of equipment or facility.

Process control system (PCS) – Operational technology (OT) systems used to operate and monitor a system or process. Examples include supervisory control and data acquisition (SCADA), primary logic controllers (PLC), and human machine interfaces (HMI).

Physical Barriers – Encompasses physical security measures in place at the water system. Examples include fencing, bollards, perimeter walls, gates and facility entrances, intrusion detection sensors and alarms, access control systems (e.g., locks and card readers), and hardened doors, security grilles, and equipment cages.

> Note: In a risk assessment, physical barriers are usually treated as countermeasures, which reduce the risk of a threat to an asset, rather than analyzed as assets themselves. However, under AWIA, community water systems must assess the risks to and resilience of physical barriers. In this case, community water systems may consider increased risks to other system assets, along with economic impacts, if physical barriers were degraded.

Pipes and Constructed Conveyances, Water Collection, and Intake – Encompasses the infrastructure that collects and transports water from the source water to treatment. Includes holding facilities, intake structures and associated pumps and pipes, aqueducts, and other conveyances.

Pretreatment and Treatment – Encompasses all unit processes that a community water system uses to ensure water meets regulatory public health and aesthetic standards prior to distribution to customers. Includes sedimentation, filtration, disinfection, and chemical treatment. For the vulnerability assessment, individual treatment processes at a facility may be grouped together and analyzed as a single asset if they have a similar risk profile.

Remote Access – The ability to access a system from a location other than where the system is physically located.

Risk – A calculated assessment of the potential for a system or asset to be damaged or destroyed by the successful exploitation of a system vulnerability by a threat.

Risk and Resiliency Assessment (RRA) – AWIA directs each community water system serving more than 3,300 people to assess the risks to, and resilience of, its system. The RRA is analogous to the vulnerability assessment of the water supply emergency plan required by NYS Public Health Law Section 1125.

Security Patches – Software updates issued to fix or patch identified security vulnerabilities.

Source Water – Encompasses all sources that supply water to a CWS. Includes rivers, streams, lakes, source water reservoirs, groundwater, and purchased water.

Standard Operating Procedures (SOP) – Step-by-step instructions to be followed for the normal operation of a piece of equipment or a facility. Allows a task to be completed the same way independent of who is carrying out that task.

Storage and Distribution Facilities – Encompasses all infrastructure used to store water after treatment, maintain water quality, and distribute water to customers. Includes residual disinfection, pumps, tanks, reservoirs, valves, pipes, and meters.

Stored Data – Data or information which is saved for later use. Data may be stored locally on physical devices such as hard drives, USB drive, or servers. Data may also be stored remotely on servers or internet (cloud) based storage.

Threat – A threat is any specific event that could impair the utility from achieving its mission. Threats can be malevolent acts, such as cyberattacks or vandalism, natural hazards, like floods or hurricanes, or critical dependencies, such as power outages.

Unique Credentials – Credentials assigned to and used by a single person for the purpose of accessing a system.

United States Computer Emergency Readiness Team (US-CERT) – Part of the U.S. Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency (CISA). US-CERT is responsible for analyzing and reducing cyber threats and vulnerabilities, disseminating cyber threat warning information, and coordinating incident response activities.

Use, Storage, or Handling of Chemicals – Encompasses the chemicals and associated storage facilities and handling practices used for chemical disinfection and treatment. Assessments under this asset category should focus on the risk of uncontrolled release of a potentially dangerous chemical like chlorine where applicable.

Virtual Private Network (VPN) – A technology which creates a private, encrypted network across a public network to enhance security.

Vulnerability – Vulnerability is the likelihood that a specific threat, if it occurs, will damage or impair the operation of a utility asset. For a malevolent threat, this value is the likelihood that an attempted attack would be successful. For a natural hazard or critical dependency, this value is the likelihood that the threat would impact operation of the utility's asset.

Vulnerability Assessment (VA) – One component of the water supply emergency plan required by NYS Public Health Law Section 1125.

Vulnerability Self-Assessment Tool (VSAT) – A tool for assessing risk and resilience at drinking water and wastewater systems. It can be used to estimate risks from malevolent threats and natural hazards and to evaluate improvements for increased security and resilience. VSAT is available from the U.S. EPA at: https://vsat.epa.gov/vsat/.

Water Information Sharing and Analysis Center (WaterISAC) – Water sector specific non-profit organization which serves as an all-threats information source for the water and wastewater sector.

Wireless Links – Method of communication or data transfer using means other than hardwired connections. Examples include radio, cellular phone, and wireless network (Wi-Fi) connections.