### **Glossary**

**Access control** Physical guidance of vehicles and people going to and

coming from a space through judicious placement of entrances, exits, landscaping, lighting, and controlling

devices (e.g., guard stations, turnstiles, etc.)

**Agency** A division of government with a specific function, or a

non-governmental organization (e.g., private

contractor, business, etc.) that offers a particular kind of

assistance.

Americans with Disabilities Act Signed into law in 1990, U.S. Public Law 101-226

prohibits discrimination based on disability, that it, the

inability to perform daily tasks using traditional

methods.

Asset Anything of value (people, information, hardware,

software, facilities, reputation, activities and

operations). Assets are what an organization needs to get the job done — to carry out the mission. The more critical the asset is to an organization accomplishing its

mission, the greater the effect of its damage or

destruction.30

Chicane A sequence of tight curves on a roadway used to slow

cars.

Clear zone An area surrounding the perimeter of a facility that is

free of shrubs and trees, and features well-maintained landscaping that does not provide hiding places for an

adversary.

**Conduit** A channel carrying something to or from a place.

**Countermeasures** A reaction to or a defense against a hostile action to

deal with a threatening situation.

<sup>30 &</sup>quot;Risk Management: An Essential Guide to Protecting Critical Assets." National Infrastructure Protection Center, November 2002.

Crime Prevention Through Environmental Design (CPTED) CPTED principles take advantage of integral features of site and facility design to enhance security by reducing the opportunity for crimes to occur. CPTED is essentially a crime prevention philosophy based on the theory that proper design and effective use of the built environment can lead to a reduction in the fear and incidence of crime, as well as an improvement in quality of life.

Criminal

An individual acting alone or in a group, using personal resources and some knowledge of utility assets, intent on economic gain. The possibility exists that a criminal may possess weapons and may inflict harm.

Cyber

Of or pertaining to the Internet, computer networks, computers, electronic communication, and other hightech related matters.

Daisy chain

Groups of padlocks connected together and hooked to a common chain in such a way as to allow access through a key that can unlock any one of the padlocks.

Debt service reserve funds

A fund in which money is placed in reserve to be used to pay debt service if there is not enough revenue to pay the debt. If the reserve fund is used in whole or part to pay debt service, the issuer usually is required to replenish the fund from the first available revenues.

Design basis threat (DBT)

The adversary against which the utility must be protected. Determining the DBT requires consideration of the threat type, tactics, mode of operations, capabilities, threat level, and likelihood of occurrence.

Detection

The point at which a potential attack is discovered, assessed, and determined to be an attack in progress rather than a false alarm.

**EPA Response Protocol Toolbox** 

A comprehensive document designed to help the water sector to effectively and appropriately respond to intentional contamination threats and incidents **Emergency Reserve Funds** A fund into which moneys are deposited to cover

extraordinary operation, maintenance, or repair

expenses in the event of an unforeseen incident such as

a natural disaster or malevolent event.

**Foot-candle** A unit of light intensity defined as the amount of light

measured on a surface one foot from a uniform point source of light equal to the light of one candle. A foot-

candle is equal to one lumen per square foot.

**Harden** To improve the physical strength of.

Improvised Explosive Device An apparatus or contraption placed or fabricated

without detailed manufacturing that incorporates destructive, lethal, noxious, pyrotechnic, or incendiary chemicals and designed to destroy, incapacitate, harass,

or distract through high-speed projectiles and

overpressure.

Improvised Incendiary Device An apparatus or contraption placed or fabricated

without detailed manufacturing that incorporates destructive, lethal, noxious, pyrotechnic, or incendiary chemicals and designed to destroy, incapacitate, harass,

or distract by creating intense heat and fire.

**Incident Command System (ICS)** A standardized response management system that is a

key component of NIMS. It is an "all hazard/all risk" approach to managing crisis and non-crisis response operations by enhancing command, control, and

communication capabilities.

**Intrusion** Entrance by force or without permission, either

physically or via electronic methods.

**Lower Explosive Limit** The lowest concentration (percent by volume in air) of

a flammable gas or vapor that can result in an explosion from ignition in a confined space.

**Lumen** The metric (SI) unit of measuring the power of light

being produced by a light source or received by a

surface.

Lux The metric (SI) unit of light intensity defined as the

amount of light equal to one lumen per square meter.

#### **Mutual Aid Agreement**

A document that formalizes coordination efforts between utilities or other agencies and facilitates the exchange of resources during an emergency. The agreement is based on the concept that resources, in most circumstances, are voluntarily provided, that there will be a reciprocal exchange if and when required, and that providing resources will not result in a profit to the providing party.

## National Incident Management System (NIMS)

A system comprising five major subsystems that collectively provide a total systems approach to risk incident management. These subsystems are the Incident Command System (ICS), Training, Qualifications and Certification, Publication Management, and Supporting Technology.

#### **Protection in Depth**

The strategy of providing multiple layers of protective measures requiring an adversary to defeat a system, travel to the next protective layer and defeat that system, and so forth until reaching the target. An example of protection in depth is the application of layers of protective measures at the site boundary (perimeter fencing system), at the building envelope (exterior walls, doors, windows, grilles, and roof system), and at the target enclosure (the room in which the targeted asset is housed).

# Public Health Security and Bioterrorism Preparedness and Response Act

Signed into law in 2002, U.S. Public Law 107-188 requires vulnerability assessments be performed and Emergency Response Plans be created or updated for drinking water systems that serve more than 3,300 people.

#### **Revolving Fund Loans**

Low interest loans provided by states to assist public wastewater systems with financing infrastructure upgrades needed to achieve and maintain compliance with regulations and to protect public health. The funds for the loans are appropriated by Congress in accordance with the Clean Water Act as amended in 1987.

Risk

The potential for realization of unwanted, adverse consequences to human life, health, property, or the environment. It is the quantitative or qualitative expression of possible loss that considers both the probability that a hazard will cause harm and the consequences of that event. Risk is usually expressed as a function of the probability that an adverse effect will occur, and the criticality of the effect on the ability to fulfill a mission or function.

Saboteur

An individual acting alone or in a group, with the intent of damaging or destroying physical assets, disrupting the utility's ability to operate and respond, and, possibly, injuring employees.

Sunshine laws

Laws that make government processes and procedures available for observation and inspection by the public.

Surveillance

The placement of physical features, activities, vehicles, and people in such a way as to maximize visibility by others during their normal activities. Surveillance may be natural or electronic, informal (office windows placed to facilitate surveillance of entry roads) or formal (continuous monitoring).

Territorial reinforcement

Physical attributes that express ownership, reinforce territoriality, and designate a gradient from public to restricted spaces. Examples include natural markers (landscaping, choke points), symbolic markers (signage, stickers), physical barriers (fences), and procedural barriers (receptionists, guards).

**Terrorist** 

An individual acting alone or in a group, with the intent of undermining stability and instilling terror through destruction of economically important or symbolic assets and by injuring and killing people. Terrorists spend considerable time and resources to select and learn about their target and plan their attacks.

Vandal

An individual acting alone or in a group, using spray paint to write graffiti or hand tools to inflict minor damage to utility assets. glossary

#### Vehicle sally port

Vulnerability

Interlocking gates within a fenced area where incoming drivers pass through the first gate and stop at the second gate. Once both gates are closed and the vehicle is captured within the sally port, a security guard may confirm the identity of the driver and, if necessary, search the vehicle to confirm the contents. Once the vehicle and driver are approved, the second gate opens and the vehicle may drive onto the facility.

A characteristic of a critical infrastructure's design, implementation, or operation that renders the infrastructure susceptible to destruction or incapacitation by a threat. Vulnerabilities may consist of flaws in security procedures, software, internal system controls, or installation of infrastructure that may affect the integrity, confidentiality, accountability, or availability of data or services. Vulnerabilities also include flaws that may be deliberately exploited and those that may cause failure due to inadvertent human actions or natural disasters. Any weakness that can be exploited by an adversary or, in a non-terrorist threat environment, make an asset susceptible to hazard damage may be considered a vulnerability.