Homeland Security

Office of Cyber and Infrastructure Analysis (OCIA)
National Protection and Programs Directorate
Critical Infrastructure Security and Resilience Note

(U) Critical Infrastructure Security and Resilience Note: Water and Wastewater Systems Sector Cyberdependencies

August 22, 2014, 1500 EDT

(U) SCOPE

(U) The Department of Homeland Security's Office of Cyber and Infrastructure Analysis (DHS/OCIA)[1] produces Critical Infrastructure Security and Resilience Notes to address emerging risks to critical infrastructure and provide increased awareness of the threats, vulnerabilities, and consequences of those risks to the Homeland. This Note informs infrastructure and cybersecurity professionals outside of the Sector about the potential consequences of cyber-related incidents in the Water and Wastewater Systems Sector and the Sector's resilience to such incidents. This Note also clarifies how computer systems support the infrastructure operations, how cybersecurity incidents may or may not compromise these operations, and the likely functional outcome of these compromises.[2]

(U) For the purpose of this Note, infrastructure cybersecurity incidents are defined as actual and potential events where a cybersecurity vulnerability is exploited by a cyberattack that can disrupt, or corrupt, normal operating conditions in computer systems, networks, industrial control systems (ICS) or process control systems (PCS), or electronic devices that control, monitor, or support the functions of infrastructure.[3] The Water and Wastewater Systems Sector infrastructure is cyberdependent in those aspects where it relies on information systems to support their physical operations and essential functions. This product focuses on the potential impacts of incidents targeting individual infrastructure systems. Complex, sophisticated scenarios with multiple distributed attacks against several key targets could have greater consequences such as overwhelming system operators and producing detrimental outcomes.

---

[1] (U) In February 2014, NPPD created the Office of Cyber and Infrastructure Analysis by integrating analytic resources from across NPPD including the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) and the National Infrastructure Simulation and Analysis Center (NISAC).

[2] (U) OCIA produces a line of informational products to deepen understanding of infrastructure. In addition to Cyberdependency Papers, other examples include: Infrastructure System Overviews, Sector Risk Summaries, and Sector Resilience Reports. These products are complementary and together help frame an integrated view of cyber and physical risks affecting infrastructure.

[3] (U) DHS and the National Institute of Standards and Technology (NIST) use the term "industrial control system" (ICS) as the generic term for all control systems that fulfill this type of function, with "process control systems" being one type, made up of a supervisory control and data acquisition (SCADA) system and programmable logic controllers (PLC). The Water Sector representatives, in writing on this topic, prefer the term "process control system" to "industrial control system" to avoid confusion. *Process Control System Security Guidance for the Water Sector*. American Water Works Association's, 2014. http://www.awwa.org/Portals/0/files/legreg/documents/AWWACybersecurityguide.pdf.

Analysis of such complex scenarios requires collaboration and resources beyond those available for this effort.

(U) This Note was developed jointly with Idaho National Laboratory, and in coordination with the National Protection and Programs Directorate's Office of Infrastructure Protection and Office of Cybersecurity and Communications, the Industrial Control Systems Computer Emergency Response Team (ICS-CERT), the National Infrastructure Simulation and Analysis Center, the Water and Wastewater Systems Sector-Specific Agency (SSA) in the Environmental Protection Agency (EPA), and representatives of the Water Sector Coordinating Council.

(U) KEY FINDINGS

- **(U) Many water utilities have industrial control systems (ICS) that are isolated from general information technology (IT) enterprise systems, but trends of increasing connectivity and automation are increasing cybersecurity risks.**
- **(U) A cyberattack may cause a brief interruption or degradation within the drinking water and wastewater services. However, water infrastructure can be operated manually in the event of an incident, preventing prolonged inoperability. There is little risk of regional or national impact to public health and the economy from a single cyberattack against a water or wastewater system.**
- **(U) A cyberattack that compromises control systems in a drinking water system is unlikely to have an immediate effect on customers, due to the existing water supply within the system. Wastewater systems do not have this buffering capacity, but prompt manual operation is likely to preclude impacts that affect anyone other than the utility.**
- **(U) Water utility IT services may be remotely operated by external entities. This could result in unsecure remote access leaving utilities unable to detect or prevent unauthorized access.**

(U) SECTOR BACKGROUND

(U) The Water and Wastewater Systems Sector represents the infrastructure security and resilience efforts of the community water systems that serve approximately 84 percent of the U.S. population and the sanitary sewage systems that serve more than 75 percent of the population.[4] Under the Safe Drinking Water Act, EPA sets standards for drinking water quality, local authorities implement these standards, and the States monitor and report on quality to the EPA for public awareness. In many cases, the States have their own regulations and the utilities must adhere to both the regulations and standards. As the SSA for Water and Wastewater, the EPA works with the States, utility operators, and representatives from water associations to

[4] (U) A community water system is a legal definition for a public water system that supplies water to the same population year-round.

ensure that the Water and Wastewater Systems Sector protection strategies are effective and practical.[5]

(U) A typical municipal water system comprises:

- (U) A source of supply
- (U) A pipeline or aqueduct to carry the water from the source to where it will be used
- (U) Raw water storage
- (U) A facility for treatment and purification
- (U) A distribution system, including treated water storage
- (U) A monitoring system

(U) A typical wastewater utility system comprises:

- (U) A means of collection (usually a network of pipes and lift stations)
- (U) Raw influent storage for sewage and industrial wastewater prior to treatment
- (U) A treatment system
- (U) Intermediate storage within the treatment system (primary, aeration, secondary and possibly tertiary treatment)
- (U) A system for releasing the treated wastewater
- (U) Solids handling and disposal
- (U) A monitoring system

(U) Most of the larger utilities in the Water and Wastewater Systems Sector have developed robust infrastructure to collect, treat, store, and distribute drinking water and to collect and treat wastewater under a variety of conditions. In general, the Sector is able to mitigate infrastructure impacts from a single cyberattack, using measures taken to strengthen infrastructure and detailed incident response procedures. Infrastructure owners and operators often require technical assistance from consultants or ICS-CERT to deal with the direct effects of a cyberattack against their computer systems.

(U) CYBER-SUPPORTED PROCESSES

(U) Water and wastewater utilities use control systems to monitor and control processes such as water production, sewage collection, water and sewage treatment, water quality sampling, water distribution, solids handling, and effluent discharge.[6] Utilities use automated environmental or access controls to manage the lighting, temperature, or access to protected areas. Cybersecurity incidents affecting these access and building control systems may increase the vulnerability of the facilities and networks they are intended to protect. In addition to these control systems,

[5] (U) Safe Drinking Water Act (SDWA) (1973, amended 1986, 1996), - http://water.epa.gov/lawsregs/rulesregs/sdwa/, accessed July 1, 2014.
[6] (U) "Roadmap to Secure Control Systems in the Water Sector," Water Sector Coordinating Council Cyber Security Working Group, March 2008. Page 11.

representatives of the Water and Wastewater Systems Sector have expressed concern for the security of computer systems used to support customer billing, potentially increasing the risk of exposing customer's personal identity and credit card information.

(U) ICS include several types of control systems, such as supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and PCS. SCADA systems are used to control geographically dispersed assets where centralized data acquisition and control are critical to system operation. In the Water and Wastewater Systems Sector, SCADA systems are used in water distribution and wastewater collection systems and in treatment plant processes, although they are often referred to as PCS because they are controlling processes. PCS use programmable logic controllers (PLC) which are computer-based, solid-state devices that control industrial equipment and processes, and remote terminal units (RTU) which integrate monitoring data and send messages within the SCADA system.[7] A DCS is an architecture that aggregates multiple distributed controllers to monitor and control localized processes, such as water and wastewater treatment.

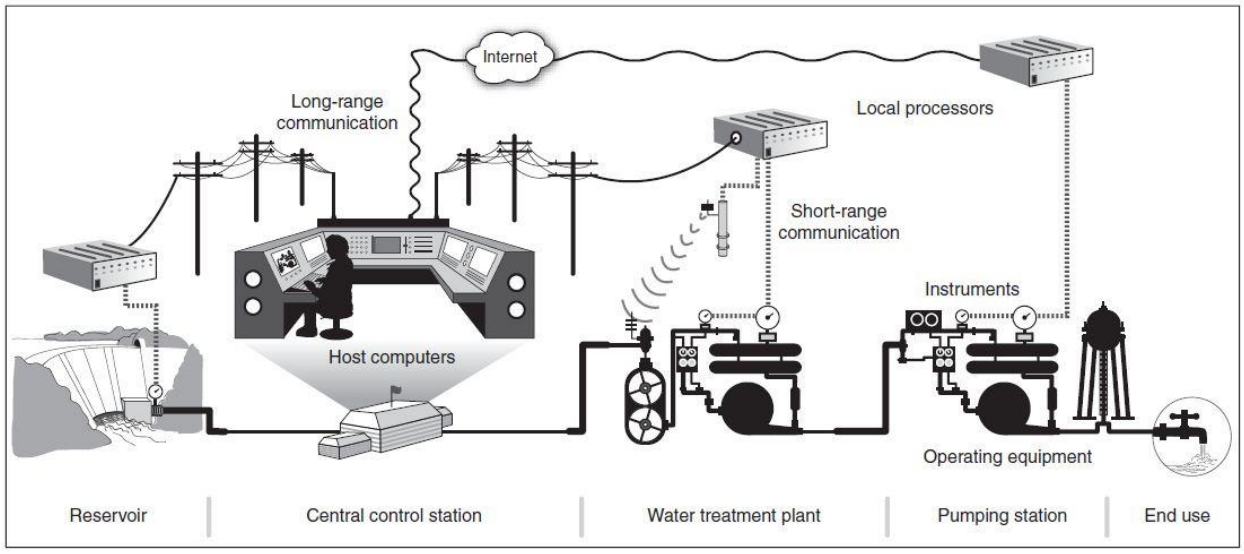
(U) ICS help verify, validate, update, maintain, and sometimes reprogram the computers that control the infrastructure functions. They enable utilities to rely on fewer staff in a centralized location to monitor remote equipment, manage treatment and distribution operations, and in most cases, control the pressures and flows of water and wastewater in pipelines. ICS provide data about raw water reservoirs or well levels, oversee flows, tank levels, or pressures in the distribution system. Additionally, ICS monitor water quality characteristics such as the pH, turbidity, and chlorine residual, and control pumps and valves and chemical dosing to the water as well as other uses.[8]

(U) Control systems are used to manage physical and automated access to systems, both onsite and remotely. A cybersecurity incident that compromises access control increases the system vulnerability from an insider attack. Someone with insider access can sabotage physical systems by manipulating control systems, or by accidentally introducing malware. Most utilities find it too costly to maintain local ICS cybersecurity expertise. Instead, utilities rely on third-party integrators, vendors, and manufacturers for equipment maintenance. Relying on third parties and providing them access to facilities and systems increases the potential for physical and cyber-related security issues.

(U) Figure 1 provides a simplified depiction of a drinking water system, illustrating the role that control systems play in monitoring and controlling storage levels in a reservoir, the movement and quality of water as it progresses through treatment processes, and the operation of pumping equipment that keeps the water flowing through the distribution system to the end user.[9]

---

[7] (U) The abbreviation RTU is also broken out as remote telemetry unit, and remote transmission unit.
[8] (U) Turbidity is the measure of relative clarity of a liquid. It is an optical characteristic of water and is an expression of the amount of light that is scattered by material in the water when a light is shined through the water sample. The higher the intensity of scattered light, the higher the turbidity. Material that causes water to be turbid include clay, silt, finely divided inorganic and organic matter, algae, soluble colored organic compounds, and plankton and other microscopic organisms. http://water.usgs.gov/edu/turbidity.htm, accessed July 17 2014.
[9] (U) U.S. Government Accountability Office, *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems are Under Way, but Challenges Remain*, GAO-08-119T, October 17, 2007.



(U) FIGURE 1—Typical Components in a Water Sector Control System (Courtesy of GAO 07-1036)

(U) Many community water systems and wastewater utilities keep ICS isolated from their IT enterprise systems.[10] Some of the Sector's cybersecurity risks have grown due to an increase in utilities' connectivity, automation, and the number of access points. These risks also increase as the systems themselves become more complex. The adoption of standards-based protocols makes potential unknown vulnerabilities more widespread. Migration of control system and other IT technologies and operating systems have also led to an increase in cybersecurity risks.[11,12] These trends are further compounded by the fact that many utility enterprise IT services are provided by a separate city or county department which limits the oversight water utilities have over their information systems and cybersecurity.[13]

(U) POTENTIAL CONSEQUENCES OF CYBERSECURITY INCIDENTS

(U) The Water and Wastewater Systems Sector has experienced cybersecurity incidents, some with operational impacts, including some with localized offsite impacts. While many utilities have been improving their cybersecurity, the current state of all Water and Wastewater Systems Sector control systems and response protocols is unclear. Not all processes that use control systems can be managed directly by operators as a backup. In isolated cases, equipment is fully automated and there is no capability to manually operate a device. Cybersecurity incidents could affect water and wastewater systems' operations in a variety of ways, the most likely consequence being short-duration denial-of-service of affected functions. Limited local adverse effects on public health are also possible.

---

[10] (U) Association of Metropolitan Water Agencies, Letter to NIST, April 8, 2013.
[11] (U) Any movement to a new IT technology, including new hardware, software, operating systems, reliance on the cloud, introduces uncertainty and possibly unforeseen vulnerabilities.
[12] (U) "Roadmap to Secure Control Systems in the Water Sector," Water Sector Coordinating Council Cyber Security Working Group, March 2008. Page 5.
[13] (U) Association of Metropolitan Water Agencies, Letter to NIST, April 8, 2013.

(U) Generally, vulnerabilities in ICS and other IT systems are compounded if there is also inadequate physical security, direct or indirect connection to the internet, or a malicious or negligent insider. Under such circumstances, cyberattacks are more likely to succeed. Water and wastewater systems being local, the impacts of the compromise would also be local.

(U) In Tables 1 through 5, OCIA has identified common Water and Wastewater Systems Sector functions that are cyberdependent and examples of potential impacts of successful cybersecurity incidents affecting these systems. Furthermore, included with these tables are records of observed incidents where infrastructure system or functional failures appear to be the result of either cyberattacks or information security problems. In addition, descriptions of infrastructure impacts caused by events other than a cybersecurity incident are included to provide examples of infrastructure failure and outcomes comparable to what could have been caused by a successful cybersecurity incident.

(U) Table 1 identifies computer systems that maintain access control data and uses the data to allow or deny access. In circumstances where water or wastewater systems facilities use digital controls to prevent unauthorized access to sensitive areas, if these controls were to be compromised, an adversary could gain surreptitious access or an authorized person could be kept out.

(U) TABLE 1—Examples of Potential Direct Effects of Cybersecurity Incidents Affecting Access Control Systems

Potential Direct Effects of Successful Cybersecurity Incidents –Access Controls				
Information Security Effect		**Loss of Confidentiality**	**Loss of Integrity**	**Loss of Availability**
Computer System Purpose	Maintains Access Control database.	Adversary has personally identifiable information (PII) and general intelligence about who has access.[14]	Adversary can provide or deny access at will.	Difficulty accessing to update.
	Compares individual's credentials to lists and allows/denies.	Adversary has PII and specific intelligence of patterns of movement.	Adversary can deny access at will.	Difficulty in operating automated access control systems or triggering alarms.

(U) Table 2 identifies computer systems that provide customer interface, specifically those that provide self-service, account management, and bill paying. When utilities provide these online services, PII is often used to control access to financial information, exposing the customer to identity theft and fraud. Cybersecurity incidents that compromise customer PII often require that the utility begin a costly process to notify customers whose information has been exposed. A utility whose systems have been compromised often bears other financial exposure and could suffer a loss of public confidence.

[14] (U) PII is personally identifiable information. Access controls sometimes require authentications at the time of establishing an account that would include PII. Customer bill-paying interfaces also expose financial information, in addition to the PII that may be used to authenticate account users.

(U) TABLE 2—Examples of Potential Direct Effects of Cybersecurity Incidents in Customer Interface Systems

Potential Direct Effects of Successful Cybersecurity Incidents – Customer Interface Systems				
Information Security Effect		**Loss of Confidentiality**	**Loss of Integrity**	**Loss of Availability**
Computer System Purpose	Maintains customer account and billing information.	Adversary has PII, financial information and knowledge about where customers live.	Adversary can manipulate accounts to avoid bills or to bill maliciously.	Difficulty accessing to update.
	Provides customer interface to allow self-service.	Adversary has PII and specific intelligence of who pays and how they pay, including credit card information.	Adversary can alter or prevent payments, or test fraudulent payment authorizations.*	Difficulty in operating online billing functions.
	* (U) This activity has been reported by Water and Wastewater Systems Sector representatives on online donation sites for contributions to local water projects. Criminals used the utility's online donation site to test stolen credit cards. While this is an example of criminal fraud using the Internet, rather than an attack on the utility itself, the protection of customer's information from theft on the utilities' websites is a concern.			

(U) Table 3 identifies computer systems that are involved in the treatment of drinking water or wastewater. Such computer systems monitor the quality of the water at different phases of treatment, report the status of the treatment operations and equipment, and execute commands that control the treatment operations.

(U) TABLE 3—Examples of Potential Direct Effects of Cybersecurity Incidents in Treatment Operations

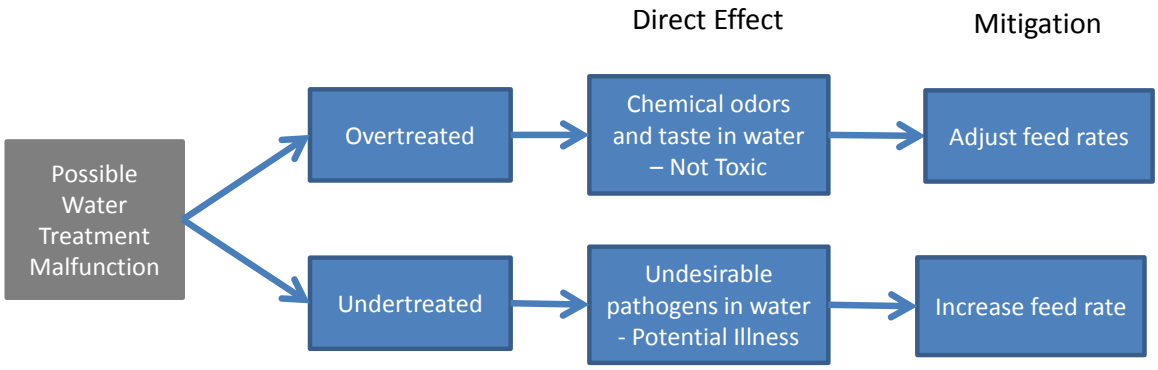
Potential Direct Effects of Successful Cybersecurity Incidents – Water Treatment Operations				
Information Security Effect		**Loss of Confidentiality**	**Loss of Integrity**	**Loss of Availability**
Computer System Purpose	Monitor water quality.	Adversary has understanding of the quality of the water.	Adversary can present a false view of the quality of the water; operators may overtreat or undertreat water.	Difficulty executing tests; difficulty communicating results or triggering alarms.
	Monitor treatment operations.	Adversary has understanding of the operation of the treatment equipment and pumps.	Adversary can present a false view of the state of equipment. Operator or automated changes may cause failures based on bad data.	Difficulty determining system or equipment status. Triggering alarms.
	Control treatment operations.	Adversary has specific intelligence about normal treatment operations at that utility.	Adversary can overtreat or undertreat water.	Difficulty in executing computer-enabled commands to change treatment operations. Treatment operations may falter.*
	* (U) In October 2006 near Harrisburg, Pennsylvania, a foreign hacker entered a water filtering plant through the Internet penetrating security and covertly used the computer system as his own distribution system for email or pirated software. The affected system controlled a vital operating function and the unauthorized activity used so much of the system's capacity, that the plant's water treatment operations were impacted. Fortunately, despite the impacts, the water treatment operations did not fail.[15]			

(U) Contributing to the potential infrastructure impacts of cybersecurity vulnerabilities is the fact that some treatment processes cannot be operated manually. Highly automated systems in some ozone and ultraviolet treatment processes that remove or neutralize contaminants have been described as not having a manual operations alternative. It is not clear how easily a utility could shift to a different decontamination procedure if these systems were compromised.

(U//FOUO) In the event of a cyberattack at a water or wastewater treatment facility, the water-quality monitoring function will typically detect whether the water has been under- or

[15] (U) Jerome, Sara. *Water Sector Eyes Federal Cybersecurity Efforts*. Water Online. July 31, 2013, http://www.wateronline.com/doc/water-sector-eyes-federal-cybersecurity-efforts-0001, accessed July 1, 2014.

overtreated. The pace of operations at water and wastewater treatment facilities would normally allow the opportunity for human operators to intervene and correct problems before there is a potential offsite impact. Figure 2 shows a simplified fault tree illustrating the potential direct effects and interventions possible with water treatment malfunctions. Levels of treatment chemicals are monitored consistently prior to the clearwell stage of treatment. The clearwell is where the water and treatment chemicals have the necessary contact for purification to take place. If there is too much chlorine, the plant simply reduces the amount that goes into the clearwell. Reporting for undertreatment of water is done in the transmission system. There could be hours', if not days' delay in water from the plant reaching the end user. This allows adjusted water to mix with the undertreated water in the transmission system.



(U) FIGURE 2—Typical Corrective Actions for Water Treatment Malfunctions

(U) If drinking water system operators are concerned about any dangerous water quality issues (chemical spills, toxic algae blooms in their reservoir, etc.) the public is notified of the problem and the proper corrective action to avoid negative health effects. While there may be treatment-related equipment that is costly to repair or replace if a cybersecurity incident results in breakage, these problems are easily identified and easy to reach. Thus, they are less costly than other infrastructure failures that may be difficult to observe in the distribution pipelines or sewerage and usually require excavation to repair or replace.

(U//FOUO) In addition to treatment operations, ICS also support the operation of water and wastewater storage. It is common for a drinking water reservoir to be positioned upstream of its service area, making it easier for the system to benefit from gravity. This also makes destructive inundations possible, if the containment structure fails. Sometimes conditions combine to cause a failure, which can be both dangerous and costly. If the structure fails, the water release can destroy the affected landscape and it can take years to restore the infrastructure.

(U) Table 4 identifies computer-supported activities for storing drinking water or wastewater. These computer systems monitor both the quality and level of the water in reservoirs and tanks, and operate the equipment used to release or retain drinking water or wastewater.

(U) TABLE 4—Examples of Potential Direct Effects of Cybersecurity Incidents in Storage Operations

Potential Direct Effects of Successful Cybersecurity Incidents at Water and Wastewater Storage				
Information Security Effect		**Loss of Confidentiality**	**Loss of Integrity**	**Loss of Availability**
Computer System Purpose	Monitor water reservoir or raw sewage storage levels.	Adversary has an accurate understanding of the levels of the reservoir or storage tank.	Adversary can present a false view leading to operator actions to retain or release when they should have done the opposite.*	Difficulty reading gauge indicators, communicating results, or triggering alarms.
	Monitor state and operation of lifts, gates, valves, and pumps.	Adversary understands the varied statuses of equipment and processes used to control levels.	Adversary can present a false view of state equipment status. Bad data can lead to faulty changes and failures.	Difficulty determining system or equipment status, triggering alarms.
	Operate equipment to increase or lower stored levels.	Adversary understands how to change the storage-supporting equipment.	Adversary can directly operate gates, divert raw water, release water or sewage, or overtop.**	Difficulty in executing computer-enabled commands to operate the lifts, gates, valves, or pumps.
	* (U//FOUO) In 2005 near St. Louis, Missouri, at the Taum Sauk Water Storage Dam, the gauges at the dam read differently than the gauges at the dam's remote monitoring station, due to a variety of operator errors.[16] The important fact under consideration is that because the equipment did not have an accurate reading, water continued to be pumped into the reservoir, overtopping it and ultimately causing a catastrophic failure releasing 1 billion gallons of water and requiring the reservoir be completely reconstructed.[17] There are no indications that this was an adversarial action, but it underscores the importance of data integrity as an information security objective in water storage control system security. ** (U) In 2000, at a sewage treatment plant in Queensland, Australia, a former employee of a software company hacked into the SCADA system releasing over 264,000 gallons of raw sewage into the surrounding environment.[18] The situation in Queensland, Australia, is completely analogous to conditions that could be found in U.S. water and wastewater systems that had not taken extra measures to prevent it.			

[16] (U) This reservoir is used to store water for a hydroelectric generation plant during peak hours, pumping water back into the reservoir during off-peak hours to be ready for the next peak demand.
[17] (U) National Weather Service Weather Forecast Office, December 14, 2005 Taum Sauk Dam Failure at Johnson's Shut-In Park in Southeast Missouri. http://www.crh.noaa.gov/lsx/?n=12_14_2005.
[18] (U) U.S. Government Accountability Office, *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems are Under Way, but Challenges Remain*, GAO-08-119T, October 17, 2007. Page 7.

(U//FOUO) The potential for an information security failure to result in overfilling is clear, however, the potential failure of a reservoir depends on the construction techniques involved in the retaining wall and the location of the reservoir in relation to the built-up environment. Not every reservoir is positioned so that the inundation resulting from this release would harm people or property. These factors may mean that the latent risk from prompt failure of a drinking water storage reservoir is low, but this has not been systematically examined. This type of destructive release would be less likely with wastewater storage, which would typically be released into local streams and rivers.

(U) Table 5 identifies activities supporting the movement of water through distribution pipelines and waste through sewage pipes that are often supported by computer systems. ICS are used to monitor the pressures and flows, and to detect the status of equipment and direct its operation.

(U) TABLE 5—Examples of Potential Direct Effects of Cybersecurity Incidents Affecting Distribution or Collection Operations

Potential Direct Effects of Successful Cybersecurity Incidents Water Distribution/Wastewater Collection Operations				
Information Security Effect		**Loss of Confidentiality**	**Loss of Integrity**	**Loss of Availability**
Computer System Purpose	Monitor the pressures and flows within the pipeline.	Adversary has understanding of the flow within the system.	Adversary can present a false view of the system. Operators or controllers may reactively do the opposite of what should be done.	Difficulty reading gauge indicators, communicating results or triggering alarms.
	Monitor the state of lifts, pumps and valves within the system.	Adversary understands the varied statuses of equipment and processes used to control flow.	Adversary can present a false view of the state of equipment. Operator or controllers reactively do the opposite of what should be done.	Difficulty determining system or equipment status, triggering alarms.
	Operate lifts or pumps to sustain appropriate system operations.	Adversary understands how to change the equipment and the effect of the equipment on the system.	Adversary can directly operate lifts or pumps, controlling material movement through the system.	Difficulty in executing computer-enabled commands to operate the lifts and pumps.*
	* (U) In 2007, in Willows, California, a failure of physical security allowed a former employee to gain access to a SCADA system and install unauthorized software which damaged the system.[19]			

(U) Wastewater collection systems typically use lifts and gravity to move waste material, while drinking water distribution systems use pumps and gravity. A drinking water system is configured to maintain several hours of water supply inside the system. Any infrastructure disruption is unlikely to result in disruption of service unless the infrastructure operations cannot be restored within the buffer. This is not true for wastewater systems, as overflows are a greater risk in general, not just from a cybersecurity incident.[20]

[19] (U) McMillan, Robert, IDG News Service, *California Canal Management System Hacked*. PCWorld, December 1, 2007. http://www.pcworld.com/article/140190/article.html, accessed July 2, 2014.
[20] (U) Information provided by Water and Wastewater Systems Sector representative contributing to this product.

(U) It is important to maintain flow in water distribution systems. If pipes become empty, the external pressure on the pipes is not balanced by an interior pressure. This may result in seepage into the pipes and contamination of the water, or fractures in older or more fragile pipes, and repairs, replacements and environmental impacts can be very costly.

(U//FOUO) While water and wastewater systems operate with computer support, and automated systems allow fewer staff to consistently and safely manage water and wastewater utilities, much of the infrastructure can be operated manually in the event of an incident. It is feasible for a single well-executed cyberattack to cause a brief interruption of drinking water and wastewater services, degrading water quality, and flooding local areas and potentially structures with water or sewage.[21] Such incidents could erode public confidence, possibly cause health concerns and potentially impede economic activity. According to Sector representatives in statements reported by the Government Accounting Office, if a single community water or wastewater system experienced repeated or recurring failures of multiple systems, this may overtax limited local staff resources, even if each failure is manageable in itself.[22] As a last resort, in the event staff cannot deal with the problem manually, if any drinking water is not adequately treated or is overtreated, there are established communication plans to notify the public that they should boil water prior to drinking or avoid drinking it altogether.[23]

(U//FOUO) Water and wastewater SCADA control systems are rarely connected to water systems beyond their utility, making it difficult for a single cybersecurity incident to propagate over a large geographical region or multiple utilities within a State. A cybersecurity incident that results in an operational disturbance in a regional water conveyance system could have a minor or unnoticed impact on the downstream service areas. There are very few regional conveyance systems, the majority of which contribute to regional balancing, rather than providing water to an otherwise unserved area. There is no reporting of cyberattacks against large-scale providers of drinking water.[24] Disruptive events are likely to be managed by operators; but, if regional systems do have a fluctuation in delivery, the downstream impacts may be quite different depending on whether this was a drinking water supply or agricultural irrigation. If a regional supplier could not deliver at the normal rate to drinking water utilities, the supplies at most community water systems would likely serve to mitigate any short-term disruptions and preclude customers from noticing a problem. Large regional irrigation systems do not have as much storage to help manage supply. In the event SCADA systems that are used to balance the distribution to various portions of an irrigation system were successfully attacked, operators would be able to intervene, and the effect on the water system may be a loss of efficiency in keeping the system balanced, rather than an inability to deliver water altogether.

---

[21] (U) While cybersecurity incidents have degraded Water and Wastewater Systems Sector operations, none have been reported to have actually caused a period of interrupted service. This remains a possibility but cannot be quantified.

[22] (U) U.S. Government Accountability Office, *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems are Under Way, but Challenges Remain*, GAO-08-119T, October 17, 2007. Page 15.

[23] (U) "Drinking Water Advisory Communications Toolbox," Page 10. http://www.cdc.gov/healthywater/pdf/emergency/drinking-water-advisory-communication-toolbox.pdf.

[24] (U) The Tehama Colusa Canal Authority (cybersecurity incident in 2007, noted in Table 5) is part of a regional system that supplies four counties in California's Sacramento Valley. Unlike the other regional systems, this is focused on irrigation.

(U//FOUO) The potential for a single cybersecurity incident to propagate too many systems is greater if an attacker infiltrates a vendor or systems integrator that supports multiple water utilities. This is because one vendor or systems integrator may provide services to several otherwise unconnected community water systems or wastewater utilities. However, the damage would be limited, since no single ICS vendor currently has a dominant share of the Water and Wastewater Systems Sector market.

(U) POTENTIAL FOR CASCADING CONSEQUENCES

(U) Individual cybersecurity incidents in the Water and Wastewater Systems Sector typically do not have offsite consequences and when they do, the consequences are unlikely to be greater than those that arise occasionally from other causes, such as equipment malfunctions or flooding. All infrastructure sectors depend on drinking water and wastewater systems to some degree, and would not be able to function for extended periods of time without water and wastewater systems. Any suggestion that there are likely to be cascading infrastructure consequences from individual cybersecurity incidents at water or wastewater infrastructure would be misleading, because a cybersecurity incident is unlikely to result in a significant denial of water or wastewater services. The potential for a temporary loss of water or wastewater services to have a cascading effect in another sector is small and localized. If an assessment is done of a particular system, or an actual incident causes a problem, it would be easy to identify other Sectors' critical assets that may be impacted. It is not possible to identify them, however, without the defining loss of service.

(U) PATH FORWARD

(U) Owners and operators recognize there are inherent vulnerabilities associated with legacy systems. Complete operating system overhaul or replacement is not practical. As the Water and Wastewater Systems Sector pursues solutions to cybersecurity vulnerabilities, they rely on other mitigations as a risk control. This insight provides context to concerns such as those voiced by James Clapper, Director of National Intelligence:

> *(U) Critical infrastructure, particularly the Industrial Control Systems and Supervisory Control and Data Acquisition systems used in water management, oil and gas pipelines, electrical power distribution, and mass transit, provide an enticing target to malicious actors. Although newer architectures provide flexibility, functionality, and resilience, large segments of legacy architecture remain vulnerable to attack, which might cause significant economic or human impact.*[25]

(U) While responding to cybersecurity incidents, Water and Wastewater Systems Sector owners and operators typically draw on external resources, such as the DHS/ICS-CERT, to deal with the cybersecurity concerns. Owners and operators will manage the infrastructure and environmental issues themselves, possibly with some assistance through existing local agreements. Although cybersecurity management, emergency preparedness, and resilience efforts can reduce the risk of a cyberattack, cybersecurity incidents still happen and adversaries continue to target Water and

[25] (U) James R. Clapper, Director, National Intelligence, Statement to the Senate Select Committee on Intelligence, January 2014.

Wastewater Systems Sector cyber assets. As recently as December 2012, researchers at the Massachusetts Institute of Technology documented active efforts of sophisticated adversaries to hack into Water and Wastewater Systems Sector control systems through a penetration of a decoy system.[26] This persistence suggests the possibility of planning more sophisticated and damaging attacks than those that target single utilities.

(U) Information sharing helps the Water and Wastewater Systems Sector become more secure, and water utilities have taken steps to work collaboratively with partners to coordinate efforts to address cybersecurity concerns. The Water Information Sharing and Analysis Center (WaterISAC) provides a secure Web-based environment for early warning of potential threats and a source of knowledge about water system security. [27] In 2012, the WaterISAC published "10 Basic Cybersecurity Measures to Reduce Exploitable Weaknesses and Attacks."[28] Additionally, in 2013 the Critical Infrastructure Partnership Advisory Council updated the "Roadmap to a Secure & Resilient Water Sector"; and in 2014 released a "Process Control System Security Guidance for the Water Sector."[29,30] These products represent a steady and coordinated effort to support efforts to reduce vulnerabilities across the Sector.

(U) The Water and Wastewater Systems Sector depends on the Federal Government to provide control system cyberthreat support and utilities call upon DHS when they suspect an incident has taken place. According to the Roadmap, by 2018 the Water and Wastewater Systems Sector is committed to improving their own capabilities to identify, understand, and disseminate timely control-system risk information both internally and among its partners.[31] If the milestones of the "Roadmap to Secure Control Systems" are achieved, by 2018 the Water and Wastewater Systems Sector will have adopted an essential body of recommended practices for control system security and established a life cycle investment and framework for control system security.

[26] (U) Tom Simonite, MIT Technology Review, *Chinese Hacking Team Caught Taking Over Decoy Water Plant*, August 10, 2013, www.technologyreview.com/new/517786/chinese-hacking-team-caught-taking-over-decoy-water-plant/, accessed July 2, 2014.
[26] (U) "Roadmap to Secure Control Systems in the Water Sector" page. 24.
[27] (U) "WaterISAC Fact Sheet," Page 1. http://www.epa.gov/watersecurity/pubs/waterISACFactSheet.pdf, accessed July 2, 2014
[28] (U) Access restricted to WaterISAC members.
[29] (U) http://www.asdwa.org/document/docWindow.cfm?fuseaction=document.viewDocument&documentid=2516&documentformatid=3187, accessed July 2, 2014.
[30] (U) http://www.awwa.org/resources-tools/water-utility-management/cybersecurity-guidance.aspx, accessed July 2, 2014.
[31] (U) "Roadmap to Secure Control Systems in the Water Sector" page. 24.