Critical Infrastructure Protection at the Local Level

Water and Wastewater Treatement Facilities

Colin Brooks
National Defense University
College of Information and Cyberspace
Washington D.C.
colin.brooks.mil@mail.mil

Abstract— The increasing number of Industrial Control System (ICS) vulnerabilities, coupled with continuing revelations about ICS compromises, emphasizes the importance of securing critical infrastructure (CI) against cyber threats [1], [2]. The ability to adversely affect the operation of an ICS through cyberspace is exacerbated by increasing use of automations and implementation of common routing protocols to communicate with control devices [3]. Local water treatment facilities are particularly vulnerable to this attack vector due to the need to manage key functions with minimal staff. Reacting to specific cyber risks without developing a holistic method to manage risk provides only a modicum of protection. This monograph demonstrates how focusing on risk management as a mitigation strategy-not individual risks-maximizes the security efforts at the local level.

Some basic IT security practices such as access control, physical security, and operations security can be applied to ICS security. However, determining which security controls to select and evaluating their effectiveness requires a process or framework that holistically considers risk across the enterprise. A risk management framework (RMF) allows an organization to assess risk in terms of impact to overall business operation: instead of assessing risks isolated to particular divisions within the organization. The National Institute of Standards and Technology (NIST) RMF, National Infrastructure Protection Plan (NIPP) RMF, and the NIST Cybersecurity for Critical Infrastruture are three complementary frameworks water facilities can employ to facilitate risk mitigation in a cost effective way [4], [5], [6], [7], [8].

Keywords—industrial control system; cyber; critical infrastructure; water treatment facilities; waste water

I. INTRODUCTION

Over the last century the position of the United States as a world leader depended on a strong economy, strong democracy, and exceptional military capability. As technological improvements increased the capability and capacity of the United States to maintain its position in the world, these improvements simultaneously created greater dependencies on critical infrastructure (CI).

According to Presidential Decision Directive (PDD) 63, CI is composed of physical and cyber assets essential to the minimum operation of the economy and the government. Homeland Security Presidential Directive (HSPD) 7 provided further details on what types of acts would compromise CI [9]. President Obama's Executive Order (EO) 13636, in concert with Presidential Policy Directive (PPD) 21(which replaced HSPD 7), expounds on the work of earlier administrations by specifically defining 16 different critical infrastructure sectors and reiterates which government agencies support each sector. Water and wastewater treatment is identified in all four Executive directives and orders as a CI sector and the Environmental Protection Agency (EPA) is assigned as the government proponent for water sector protection in HSPD-7 and reiterated by PPD 21. [10]; [11]; [12]

Water and waste water treatment is essential for clean drinking water, preventing disease, and protecting the environment [13]. Efforts at the beginning of the 20th Century were primarily aimed at ensuring purity of drinking water. In the late 1990s and early 21st century, the importance of protecting water sector resources from malicious actors was recognized as a security priority as awareness of vulnerabilities grew [14].

Particular concern about vulnerabilities in Industrial Control Systems (ICS)—the systems responsible for controlling CI operation (figure 1)—increased as experts identified the possibility of exploiting vulnerabilities remotely through Internet [1], [2]. ICSs are composed of a number of different devices including: Supervisory Control and Data Acquisition (SCADA), Human Machine Interface (HMI) devices, Radio Terminal Units (RTU), Main Terminal Unit (MTU) and Programmable Logic Controllers (PLCs), each of which have vulnerabilities. Increased use of common routing protocols to communicate with these devices exacerbates the issue of ICS cybersecurity [3].

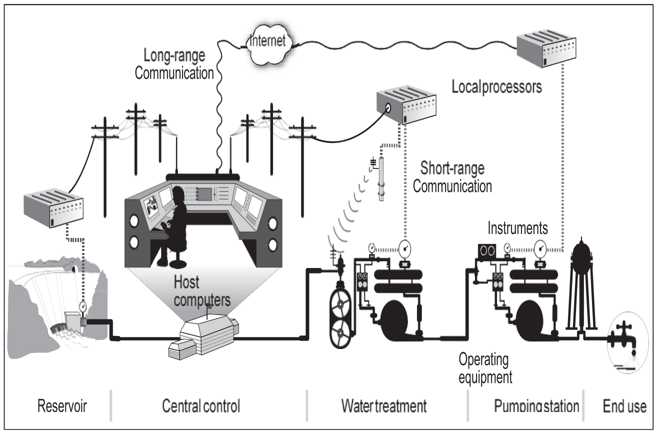


Fig. 1 Components of a control system in water treatment and distribution facility (p.3) [31].

Local water facilities are particularly vulnerable to this attack vector due to the need to manage key functions with minimal staff. Reacting to specific cyber risks without developing a holistic method to manage risk provides only a modicum of protection. Adding to this challenge, local water sector facilities have aging equipment, limited budgets, and only have a small number of personnel whose primary purpose is to operate and maintain equipment—not to provide security. Given the proliferation of cyber threats and limited resources available to local water facilities, it is still possible to reduce risk and improve the security posture. This monograph demonstrates how focusing on risk management as a mitigation strategy-not individual risks-maximizes security at the local level.

Threats and vulnerabilities to ICSs are discussed in the first section, showing the increasing feasibility of attacks and highlighting the vulnerability of water sector facilities. The National Institute of Standards and Technology (NIST) Risk Management Framework (RMF), National Infrastructure Protection Plan Risk Management Framework (NIPP-RMF) and the NIST Cybersecurity Framework for CI are then reviewed. These frameworks provide a construct for local water facilities to reduce risk. Resources available to assess risk and how to apply security measures to greatest areas of risk based on a RMF are next discussed. The conclusion shows how the use of a risk management framework enables local water facilities to apply limited resources to best effect [4], [5], [6].

II. THREATS AND VULNERABILITIES IN ICS

Many different CI sectors have been adversely affected through cyberspace. Disruption to air traffic control systems in Worcester, MA in 1997 was caused by a teenager disabling part of the phone network. In 2000, a disgruntled contractor at the Maroochy Shire Water Treatment facility in Australia caused hundreds of thousands of gallons of sewage to flow into streams by controlling facility equipment from a laptop computer. In 2003, the Structured Query Language (SQL) worm Slammer, disabled safety monitoring systems at the Oak Harbor, OH nuclear power plant for nearly five hours [15].

Recent findings by members of both the public and private sector exacerbate the concern over the vulnerability of ICS to attack. In 2016, the Industrial Control System-Computer Emergency Response Team (ICS-CERT) of the Department of Homeland Security (DHS) found 700 security vulnerabilities in the 300 systems it analyzed [16]. Positive Technologies, Inc., a network security company, identified 197 vulnerabilities in ICS components of major manufacturers in 2017 [17].

In late 2017, Schneider Electric, a major manufacturer of ICS components, revealed its components were compromised by hackers. The malware, labeled Triton, was a zero-day (previously unknown) vulnerability in the Triconex Tricon safety system firmware. The malware escalated privileges and then dropped a remote access tool (RAT) in the system to await further instructions. The RAT was intended to manipulate emergency shutdown processes to keep the system operational, allowing further invasive action. Triton continued system analysis and reconnaissance as it worked, exfiltrating information back to the source. It was unclear who was responsible for the attack, but it demonstrated an elevated level of sophistication [18].

In 2010, the malicious code known as Stuxnet was revealed as the cause of the degraded capability of the Iranian nuclear refinement facility at Natanz. Specifically, it attacked Siemens PLCs that controlled the centrifuges, causing them to spin at erratic rates [19]. It is widely considered the first confirmed act of cyber war and is believed to be an effort of the U.S. and Israel to thwart the Iranian nuclear weapon development program [20]. This initially generated a great deal of excitement in the IT community, but many members of the ICS sector believed it was not important to their operations as it targeted centrifuges belonging to Iran, not US infrastructure [1].

While cyber threats to CI in general are more prevalent in the last two decades, there is a long history of attacks on the water sector. During World War II, the Japanese poisoned Soviet water sources with typhoid bacteria; Soviets flooded the area south of the Istra Reservoir near Moscow to slow the German advance in 1944; Israeli water infrastructure was attacked by Yasar Arafat's Fatah in 1965; neo-Nazis attempted to poison urban water supplies in the U.S. in 1972; and two Al Qaeda operatives were arrested in 2002 with plans on how to poison U.S. water systems [21], [22].

Fear of terrorist attacks, especially on water facilities and water supplies, increased in the 1990s and early 2000s, leading to formalized efforts to protect CI. In 1998, PDD-63 aligned federal agencies with particular infrastructure sectors to better coordinate protection efforts. PDD-63 established Information Sharing and Analysis Centers (ISAC) for public-private security cooperation to facilitate threat data sharing between the government and the private sector [10]. In response to the 2001 terrorist attacks, the Bush Administration passed the *Public Health Security and Bioterrorism and Response Act of 2002.* It directed vulnerability assessments of critical infrastructure be conducted in each sector, allocated funding for protection of water sector facilities, and increased penalties for attacks on water [23], [24], [10].

Water is a particularly vulnerable resource. Approximately seventeen percent of the drinking water treatment facilities in the U.S. provide service to ninety-two percent of the populous [13]. This means a terrorist or other malicious actor targeting one of approximately 2,700 facilities could have an inversely proportional impact on public health, and may be able to delay detection of a compromise. One way to execute an attack is to introduce toxic substances through a service point (a fire hydrant, for example) via backflow. Backflow occurs when the pressure gradient of the water in the distribution system is overcome by a source with higher water pressure (Figure 2). This can accidentally occur when backflow prevention devices, like check valves, fail due to wear or non-malicious acts [25].

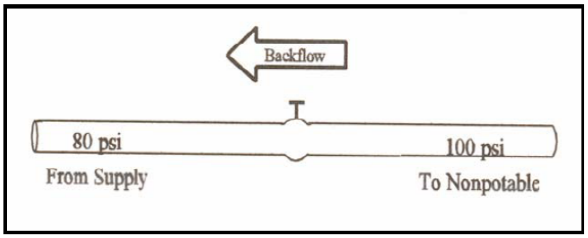


Fig. 2. Backflow due to Backpressure [25].

There are numerous examples of such accidental incidents, including: a glycol contamination of a West Virginia county health department due to faulty check valve; failure of a backflow preventer on an elementary school boiler feedline causing drinking water contamination; and ironically, at a Boston hotel in 1974 where a conference of the American Water Works Association was being held. Chromium entered the drinking water through a submerged inlet cross-connection to the building air conditioning system [25].

Backflow devices are designed to prevent accidental contamination but can be defeated by a determined attacker and are not a reliable safeguard against malicious actors. To attack through backflow only requires the actor to overcome the ambient water pressure with a pump capable of creating a higher pressure and injecting a contaminant. If injected correctly, a contaminant can be carried throughout the rest of the system from a strategic point. Using a highly toxic contaminant only requires a few gallons to be introduced to have widespread impact. Devices to detect contamination are not ubiquitous and could be modified to cause a false negative for personnel monitoring them [22].

As shown in Figure 3, a marked increase in attacks on water sector ICSs occurred from 1999-2012. Although some of the upward trend can be attributed to late disclosure or to better detection of vulnerabilities, the increasing number of ICS equipment able to be accessed remotely makes them more vulnerable to attack. In the US, the connection of ICS components to the Internet has increased by ten percent from 2017 to 2018 [17].

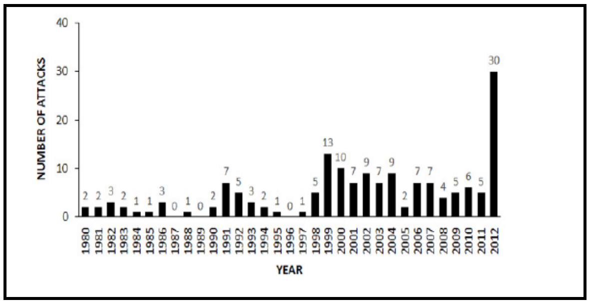


Fig. 3. Recorded trends on water critical infrastructure (p.4) [21].

Further compounding the issue is the recent development of system control applications for mobile platforms. It improves the productivity and efficiency of local water facilities but exposes ICS to cyber threats not previously encountered [26]. For example, Bolshev and Yushkevich found 147 vulnerabilities in 34 vendor applications used for managing ICS components [3]. Another research team, Rios and McCorkle, set out to find 100 security flaws in ICS software in 100 days but found 665 flaws in the same amount of time: seventy-five of the flaws were easily exploitable. The latter team's research was all based on open source information from the Internet. [27], [1].

Terrorists are not the only ones who could exploit such ICS vulnerabilities. Cybercriminals may target the systems because they are less secure and serve as a means to another end. In 2006, a computer used for controlling water system devices in Harrisburg, PA was compromised and used for spam e-mail distribution [28].

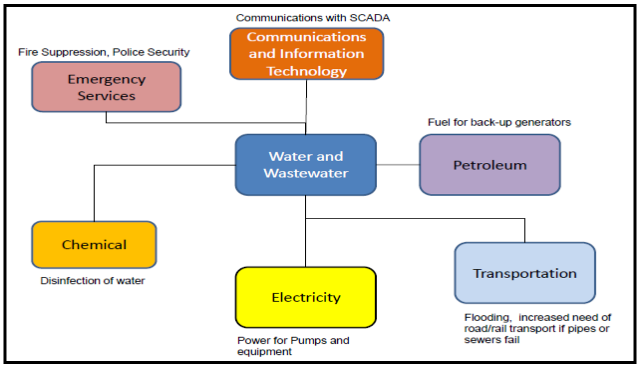


Fig. 3. Dependence of the Water Sector on other CI (adapted from [21]).

Feasible attacks on water sector assets through cyberspace are only one facet of a complex security problem. Interdependency between the water sector and other CI sectors amplifies the potential for catastrophic damage (see Figures 4 and 5). The water sector depends on CI such as electricity to operate pumps, petroleum for backup generators, and the chemical sector for disinfection of water. Conversely, other CI sectors need water for manufacturing, cooling equipment, or agricultural production.

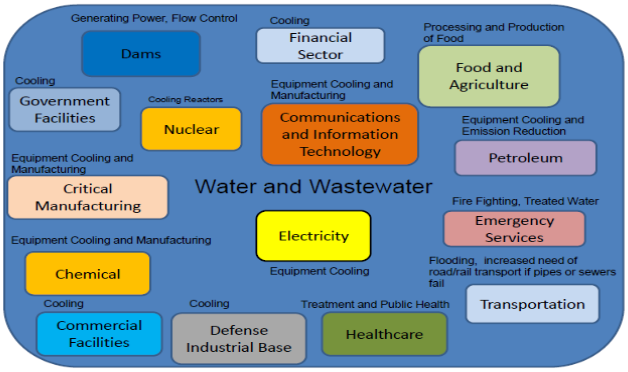


Fig. 5 Dependencies of other critical infrastructure on the water sector (adapted from [21], [38], [11] [33]).

Denial or disruption of water service can have cascading effects. For example, an uncontrolled release of a large volume of wastewater, as happened in Australia in 2000, could have catastrophic effects on public health, environmental well-being, and commercial facilities [29]. Attacks on transport systems used to pipe water from sources to agricultural production could cause significant financial harm [24]. Catastrophic damage to water mainline pipes by opening and closing main gates too rapidly, causing a hammering effect, could collapse sections of pipe, immobilizing traffic and delaying emergency service response time-furthermore, it could cause backsiphonage (Figure 6).

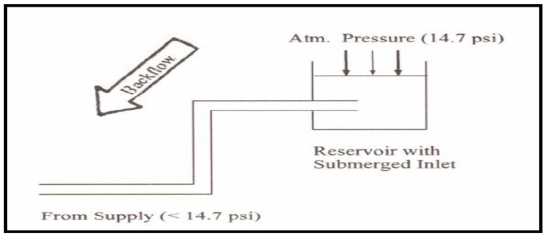


Fig. 6 Backsiphonage [25].

Backsiphonage is a type of backflow caused by a zone of negative pressure in a water system—if a cross-connection exists, atmospheric pressure pushing against a contaminant will force it into the water supply that contains zero negative pressure [25]. These types of attacks on distribution systems or use of them for attacking other CI, is a concern expressed by many in the sector [30], [31].

III. CHALLENGES TO SECURING THE WATER SECTOR

Securing facilities from cyber threats is challenging for many reasons. These include funding, the age of equipment, and education [1], [8], [31]. One of the main challenges water sector decision makers face in securing their facilities is obtaining enough funding. The amount of funding can vary depending on the size of the facility and the number of people serviced. Larger facilities have better opportunities to account for security in planning their budget because they are better resourced than smaller ones [2], [32].

Though serving fewer people than a large urban area, denial of service to a rural facility could have equivalent impact by degrading public confidence in water supplies and other second and third order effects. These could include pressure on local and state government to provide potable water for extended periods of time, decreased revenue from business and tourism, and disruption to agricultural and manufacturing operations [33], [27], [2], [21], [26].

Most of a local water facility budget is earmarked for operations and maintenance. The Congressional Budget Office (CBO) noted 67% of funding for water infrastructure is spent on operations and maintenance by state and local government [8]. Such a limited budget for efforts other than infrastructure maintenance requires conscious decisions to invest in security by facility and sector leadership. Therefore, efforts by local water facilities to implement monitoring software or hardware security appliances may be limited or impractical.

Another factor in securing ICS is the age of the equipment. Securing SCADA, PLCs, and HMI is challenging because much of it is twenty to thirty years old and designed with reliability and safety in mind, not security [1], [8], [31]. Systems initially used obscure, proprietary protocols for communication and were isolated from other early computer systems. "Security through obscurity" was a common approach [14]. The growing interconnections between previously isolated systems and the Internet, along with use of common protocols, like Transmission Control Protocol/Internet Protocol (TCP/IP), expose ICSs to previously unidentified threats [3]. Like use of mobile computing platforms, using newer technologies to manage equipment designed before the advent of the Internet poses risks.

Some gaps in ICS security exist due to lack of awareness of cyber threats and their impact to operations. An example is the focus on cybersecurity of information technology (IT) (corporate network) versus operations technology (OT) security. Engineers understand the process flow and operation of ICS components but are often not aware of the vulnerabilities in their connected systems. Conversely, IT personnel often do not understand the unique nature of SCADA systems and how patching vulnerabilities might interfere with system processes [1]. Reviews by the National

Cybersecurity and Communication Integration Center (NCCIC) identified common network issues such as improper use of virtual machines, poor configuration of Virtual Local Area Networks (VLANs), improper management of Bring Your Own Device (BYOD) implementations, and, where IT and OT efforts were combined, OT was often unmonitored [34].

Staff at a local water facility in New England interviewed by this author corroborated many of challenges noted in other reports and studies. They stated their operation was largely dependent on revenue from the businesses and households they serviced. Much of the revenue was reinvested in maintaining the infrastructure while the majority of the budget allotted for waste water treatment was spent on removal and incineration of sludge. Most of the pump stations dated to the 1980s and remote connectivity to the system was limited, but possible through the telephone system. While the operators and supervisors were highly skilled at their jobs, understanding how cyber threats associated with an IT network could affect an OT network was less developed.

IV. MANAGING RISK

In light of these vulnerabilities and challenges, steps can be taken to advance the security of the water sector. Some basic IT security practices such as access control, physical security, and operations security can be applied to ICS security. However, determining which security controls to select and evaluating their effectiveness requires a process or framework that holistically considers risk across the enterprise. An RMF allows an organization to assess risk in terms of impact to overall business operations, instead of assessing risks isolated to particular divisions within the organization. The NIST RMF, NIPP RMF, and the NIST Cybersecurity for Critical Infrastruture are three complementary frameworks a water facility can employ to facilitate risk mitigation in a cost effective way [13], [4], [29], [35], [36], [37].

A. NIST Risk Management Framework

The NIST RMF was developed to improve information security, strengthen risk management processes, and encourage reciprocity between federal agencies. It is a holistic approach to risk, incorporating IT security into enterprise risk management, emphasizing continuous monitoring and linking risks to organizational and executive level operational decisons. It is the successor to the Department of Defense Information Assurance Certification and Accreditation Process (DIACAP). DIACAP emphasized compliance with patching of system vulnerabities whereas the RMF broadly considers many facets of information system security [6].

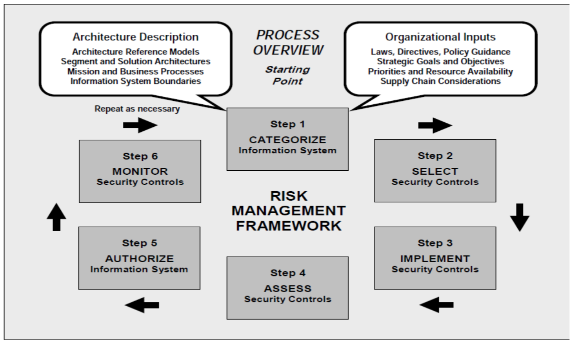


Fig. 4 NIST Risk Management Framework [4].

The NIST RMF consists of six steps (Figure 7). Step one categorizes the system and information processed based on an impact analysis. The second step identifies a set of basic security controls based on categorization—tailored to the organization assessment of risk. Step three implements the selected security controls, documenting how they were deployed. The fourth step assesses the security controls to determine effectiveness in meeting security requirements. Step five authorizes system operation based on determination of acceptable risk to operations, assets, individuals, and other organizations. The last step is continuous monitoring of controls for effectiveness, documentation of changes to the system or environment, and report of security state to organization officials [38].

The NIST RMF is a baseline framework that can be applied to both governmental and non-governmental organizations [38]. The process can be applied to any type of IT system. It does not consider specific types of systems.

B. NIPP Risk Management Framework

The NIPP-RMF is specifically designed with CI in mind. Presented in the 2013 National Infrastructure Protection Plan, it recognized the importance of a public-private partnership and the differing constraints on private versus government organizations [5]. NIPP-RMF is broad in its application, accounting for dissimilar operating environments and both natural and man-made threats. It emphasizes the importance of information sharing to build resilience and improve threat reduction. Figure 8 provides an outline of its main components [5].

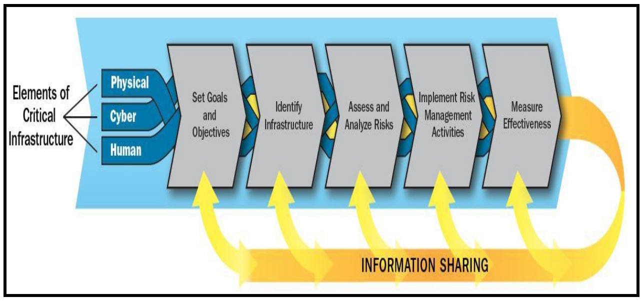


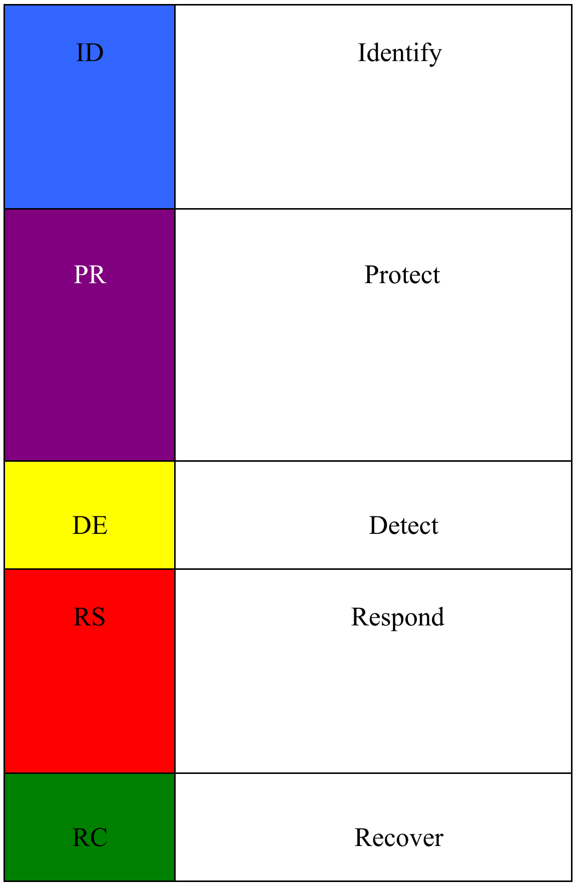
Fig. 8 NIPP RMF [13].

The NIPP-RMF complements other efforts such as the Threat and Hazard Identification and Risk Assessment (THIRA) process conducted by regional and urban jurisdictions to establish capability priorities [5]. The CI community shares information and builds upon best practices and lessons learned to fill gaps in security and resilience through the RMF.

The first step is set at the national level with input from each CI sector. The second step includes identification of all assets, systems, and networks for continued operation, considering dependencies and interdependencies. Step three, assess and analyze risks, relies on analysis of threats, vulnerabilities, and consequences. Information sharing is essential in this step. Step four, implementing risk management strategies, involves prioritization of activities to manage risk based on costs and potential to reduce risk. The final step in the process measures effectiveness of controls. Continuous monitoring is essential to the risk management process, informing leadership if the controls in place are effectively mitigating risk [5].

C. Cybersecurity Framework for Critical Infrastructure

The Cybersecurity Framework for CI is a risk management construct developed specifically for CI cybersecurity by NIST and numerous stakeholders in the private sector. It is composed of three distinct sections including: The Framework Core, Framework Implementation Tiers, and Framework Profile [6]. The Framework uses holistic business risks as drivers for cybersecurity activity instead of the compliance related endeavors previously associated with cybersecurity [39]. Integrating cybersecurity with the overall process of business operations informs decision makers where they can best apply resources to enable operations.



ID	Identify
PR	Protect
DE	Detect
RS	Respond
RC	Recover

Fig. 9 Function identifiers [6].

The functions of identify, protect, detect, respond, and recover are part of the Framework Core and provide a strategic view of the lifecycle management of cybersecurity risk. The Core provides a method for communicating industry standards, guidelines, and practices across the organization from strategic level to operational and tactical levels. It identifies key categories and subcategories for each function and correlates them with existing guidelines and best practices for desired outcomes. The five primary Core categories are shown in Figure 9 [6].

Framework Implementation Tiers define how an organization views cybersecurity risk and how it manages risk. It describes the level of management from reactive, to adaptive and agile. This permits an organization to see itself and determine how risks are managed. For instance, intrusion detection and response may have a well-developed process while a natural disaster contingency may have little planned response action, giving them an assessment of agile in the first instance and reactive assessment in the second. Identifying differences in response level informs the Framework Profile [6].

The Framework Profile represents the outcomes based on the business needs selected from the Framework Categories and Subcategories. Profiles can be used by an organization to identify areas for cybersecurity improvement. Profiles can inform the current state of security and present a desired end state. Based on the gaps between current and end state Profiles, the organization can assess risk and allocate resources based on what is most important for business operations [6].

Implementing the Framework is not without challenges. The Government Accountability Office (GAO) found many CI sectors have not implemented the Cybersecurity Framework due to lack of resources, lack of knowledge and skills to implement it, or regulatory and industry requirements preventing implementation. Some CI sectors had concerns over disclosure of vulnerabilities or other priorities such as physical security or direct support to customers. Some sectors perceived no cyber threat at all and believed there was no need to use it [32].

While some of these arguments are relevant, it indicates a lack of knowledge of the Framework purpose and intent. The Cybersecurity Framework for CI clearly states [6]:

> The Framework complements, and does not replace, an organization's risk management process and cybersecurity program. The organization can use its current processes and leverage the Framework to identify opportunities to strengthen and communicate its management of cybersecurity risk while aligning with industry practices. Alternatively, an organization without an existing cybersecurity program can use the Framework as a reference to establish one. (p.4)

The ability to address cybersecurity concerns within a limited budget with personnel that are primarily involved in operating facilities or performing IT functions is difficult at best. The Framework maps to industry standards, without dictating which ones a facility must use. How leadership applies the resources they have depends on the risks they identify and their perceived threat to business operations.

V. PRACTICAL TOOLS FOR ASSESSING RISK

Risk assessments are critical in determining where the greatest vulnerability and return on investment is for a facility. All three frameworks call for assessing risk. Several tools are available to water facilities at no cost, to help them practically identify and mitigate risks. Some of these tools are automated programs that map the network to help operators understand the flow of data while others are computer driven queries that populate a spreadsheet with recommended best practices. Several of these tools are discussed below [40], [41].

The Cybersecurity Evaluation Tool (CSET) is a free, downloadable desktop software that guides operators and system owners through a step-by-step guide to assess cybersecurity practices [40]. It correllates answers obtained through queries to accepted industry practices for securing networks. Data entered into the system is protected by the Protected Critical Infrastructure Information Program (PCII). This enables private sector entities to pass information to DHS without fear of litigation or public disclosure [40].

The Vulnerability Self-Assessment Tool (VSAT) is a water sector specific tool developed by the EPA to help water facilities identify areas of most vulnerability and find the most cost effective measures to reduce those risks [40]. Like CSET, it is freely downloadable, but can be run from a web browser. Data is not retained by the EPA, protecting sensitive information about individual facilities.

A third tool is the Design Architecture Review (DAR) assessment. It reviews network architecture and security controls, looking at data flow, communication sharing, and proper communication channels [42]. The Network Architecture Verification and Validation (NAVV) assessment, another type of review, passively monitors data traffic to determine if there are leaks across boundaries and identifies anomalous behavior [40]. Neither of these assessments requires connection to the OT or IT network at a facility.

National Cybersecurity Assessment and Technical Services (NCATS) is a team that can conduct penetration testing to test the security measures implemented by a facility. This is a valuable resource to determine if measures put in place after a security review are effective: achieving Step 5 of the NIPP-RMF [40].

The Cyber Resilience Review (CRR) is a sixth type of assessment freely available through DHS. It can be done as a self-assessment program or facilitated by DHS experts. It is designed to help organizations use the Cybersecurity Framework. It addresses efficiency by balancing risks and costs; provides a roadmap by determining the best standard for an organization to use; and addresses internal and external challenges of an organization [43].

The risk assessment tools outlined above, are free of charge. As an example, VSAT can be used to assess risk and increase the security posture of a facility. Beginning with the choice of quantitative or qualitative method for assessing risk, it leads a user through specific questions about the water utility—including assets, countermeasures, and threats. The current risk to the facility based on threats/assets input and existing countermeasures is provided as an output. Improvement recommendations are presented after completing the baseline assessment and a cost/risk analysis is used to develop new packages of countermeasures that conform to existing budgets or can be executed over a period of time. Finally, it can generate reports of the analysis results developed around the inventories of assets, threats, and countermeasures

The tool has a demonstration mode with pre-filled data to enable new users to understand the relationship between different values and the impact on operations if a component fails or is attacked. Key parameters and areas within the tool to input data are outlined below.

The Asset Selection Screen is where facility specific assets can be selected for analysis. This is pre-populated with common assets such as generators, pumps, wells, instrumentation, and valves. Customization can be done by editing existing assets for system specific items.

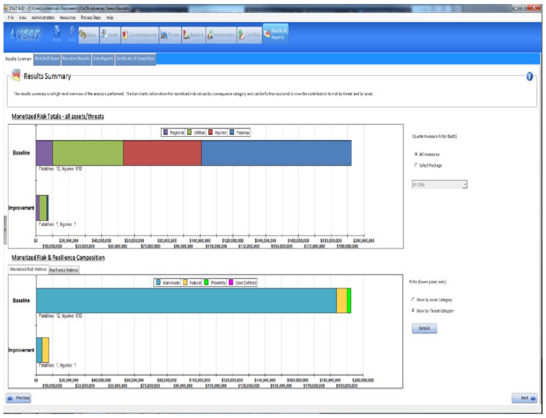
The countermeasures section of the VSAT allows user defined countermeasures to threats to be entered. Similar to the asset selection, it is populated with common countermeasures. The countermeasure inputs, along with the asset inputs, form the baseline risk assessment for the facility. Unique inputs can be added to the countermeasure screen to tailor to the specific situation of a water facility.

The Baseline Analysis performs analysis on one asset/threat combination at a time. It indicates the relative financial cost of a compromise. It queries the ability to reduce the consequence levels of an incident given the ability to detect, delay, or respond. The system asks for the likelihood of occurrence and, combined with the previous responses, provides baseline risk and resiliency metrics.

Subsequent queries request potential improvements to existing countermeasures and likelihood of damage if a vulnerability is successfully exploited. This provides results of cost savings and reduced likelihood of damage, expressed as a percentage. It allows a facility to compare its existing security posture to future posture if countermeasures are improved and displays this a monetized amount of risk reduction.

Finally, the Results and Reports section summarizes the vulnerability assessment. It can represent the data in a narrative format or as a chart. It can display the monetized risk metrics and resilience metrics of the assessment. The

Results section may be used to drill-down on the specific risks related to an asset/threat combination. Figure 10 shows the monetized risk output associated with the threats and vulnerabilities and other data input in the earlier portions of the query.



Results Summary

The results summary is a high-level overview of the analysis performed. The bar charts below show the monetized risk values by consequence category and can be further explored to view the contribution to risk by threat and by asset.

Fig. 10 Results Summary [44].

On the whole, the water sector has done more assessments to identify vulnerabilities than any other sector [42]. While this places water and wastewater facilities ahead of peer CI, the challenge of securing decades old SCADA equipment remains.

VI. PRACTICAL WAYS TO IMPLEMENT AN ACTION PLAN

Based on the assessment results, decisions can be made about which areas are most important to address. In reality, a local facility will still have a small budget for security and may not be able to apply resources to some areas highlighted as a risk —nor have the operational capacity to maintain them over the long term. However, some security improvements can be made at low cost.

Information sharing and coordination is an area where risk management gains can be made with minimal effort. Free information updates from organizations such as the Water Information Sharing and Analysis Center (WaterISAC) are available for water facility managers to stay abreast of trends in cyber threats [44]. Coordinating with local emergency services, critical partners (such as electric service providers), and public health agencies prior to an incident can improve response and recovery operations [45].

Training, education, and coordination are first steps but implementation of software, hardware, and physical security requires finesse. OT and IT networks have similarities but the specialized nature of ICS equipment sometimes prevents patching or other standard IT security measures from being implemented [7]. Updating ICS by replacing old equipment in wholesale fashion is not feasible for most facilities [14]. Costs associated with expansive security software and hardware implementation are often prohibitive for local facilities [8].

Using technology such as pre-processors can be an inexpensive and effective way to reduce some common risks to water sector ICS (Figures 11 and 12). Researchers at the University of Louisville demonstrated this concept in 2012. A pre-processor is a security module built on a small circuit board that is placed before a field SCADA device with either a software interface at the HMI point or another board in the same location to allow control of the field unit. This does not require replacement of equipment being added in-line to existing architecture. A Gumstix® circuit board was used in this experiment with the cost of only a few hundred dollars [7], [48].

The device provides authentication and authorization on behalf of the SCADA device. By configuring the Modbus protocol—a common protocol used in ICS—to incorporate a connection request, challenge, and challenge-response and incorporating Role Based Access Control (RBAC), users are only able to perform functions for which they have authorization (see Figures 11 and 12). The device uses a simple operating system (OS) known as OKL4 to reduce overhead. Further research by Schreiver indicates a Bloom filter is a viable option for enforcing RBAC and limits the amount of bandwidth required to operate [7], [48].

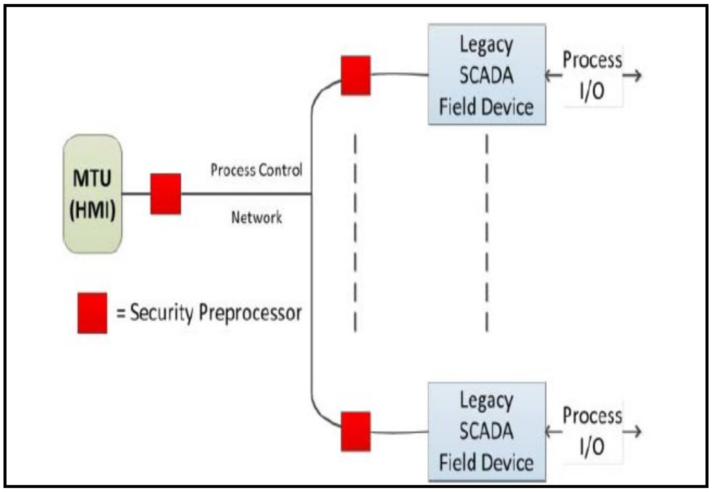


Fig. 11 Pre-processor integrated with ICS architecture [7].

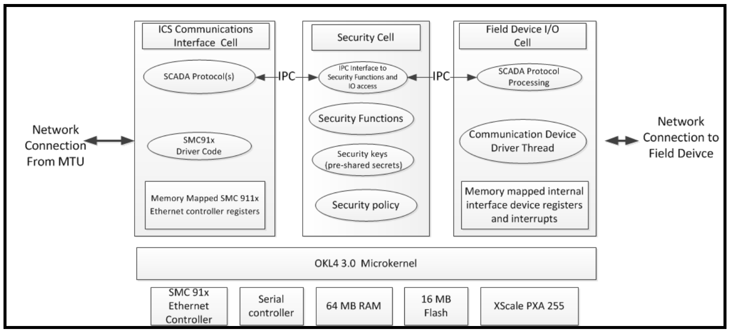


Fig. 12 Pre-processor architecture [7].

VII. FIELD IMPLEMENTATION

The implementation of the Cybersecurity Framework and the tools previously highlighted by water and wastewater treatment facilities has varied. In the February 2018 report on Framework implementation by the GAO, the EPA reported it does not have the statutory ability to collect information on implementation of the Framework by the water sector and had no plans to implement a methodology to do it. [32]

This perspective was not unique to the water sector. A dearth of information on Framework implementation was ubiquitous across all 16 CI sectors [32]. The water sector is the most proactive of the CI sectors to leverage assessment resources, however. From 2009 to 2014, 128 onsite assessments were conducted by the sector—double the number conducted by the next closest sector in the same amount of time [43].

Reasons for not leveraging security assessment tools at the local level included: lack of awareness of tool availability; limited understanding of cyber threats to the facility or sector; lack of personnel to dedicate to conducting security risk assessments; reluctance to share sensitive information; and absence of directives from higher echelons to implement risk assessments [32], [2]. The primary focus of the facilities is provide the service for which they are mandated. While importance of security was not entirely ignored, being able to simply execute the mission of water reclamation or purification was prioritized over other activities. Time to dedicate to security considerations limited. [32], [52]

One local facility manager who was interviewed, depended on the state to manage security concerns. The manager was unaware of WaterISAC or the tools available. While the importance of security was not misunderstood, daily operations had primacy.

In 2015, the EPA published results of a pilot test of a contamination warning system (CWS) conducted jointly with five different water utilities across the U.S. Its purpose was to determine timely detection and response to drinking water contamination. Cybersecurity was an important component of the program, with emphasis on detection of contamination (with a minimum of false positives), operational reliability, and early detection to improve response time. [32], [52]

The report highlighted the importance of communicating the value of the program to personnel and the impact to daily operations and how it enhanced core job functions. Support from senior management, education of key leaders, and inclusive engagement across the staff were particular lessons learned. In the latter instance, it was discovered one pilot site did not engage their IT personnel and found the design of the information system was infeasible because it conflicted with IT requirements. While the report focused on a CWS, the challenges of incorporating the multiple facets of a new process is applicable to instituting and assessing cybersecurity at the local level of the water sector. [52]

VIII. CONCLUSION

The increasing number of ICS vulnerabilities identified by researchers and industry experts coupled with continuing revelations about ICS compromises emphasizes the importance of securing critical infrastructure. Security of water sector ICS is undeniably important in its own right but also for other CI sectors. It is necessary for safe drinking water, environmental safety, growing food, cooling equipment for businesses and hospitals, and manufacturing.

As water sector ICS increasingly leverage routing protocols and automation equipment to reduce manning requirements and increase productivity, potential for system vulnerability exploitation will occur. Evolving threats to water CI through cyberspace places an increased burden on local water facilities to protect their resources. They are especially challenged as they often do not have the training or equipment to identify and mitigate the risks to their systems. They may be able to apply only limited risk reduction measures by allocating personnel, funding, and materiel against specific threats.

Defending water sector ICS from attack cannot be viewed as a separate function, relegated to IT personnel or system operators, but must be viewed as part of a whole of business approach to risk. Leveraging the NIST RMF, NIPP-RMF and Cybersecurity Framework for CI as a methodology for categorizing cyber risk, will aid organizations in holistically viewing risk across the enterprise. It aids in allocating resources to achieve greatest return on investment.

Several assessment tools exist to help executives and operations personnel apply the principles of the NIST RMF, NIPP-RMF, and Cybersecurity Framework CI. Some, like CSET, CRR, and VSAT, can be performed at a local level without external support. Others, like NAVV and DAR, are facilitated by DHS at no cost to the local facility and help identify vulnerabilities on the network and areas for improving network security. Some cost effective measures such as installing pre-processors at legacy water sector facilities to prevent unauthorized system access can be done.

Using the NIST RMF, NIPP-RMF, and the Cybersecurity Framework for CI with best network security practices, local water sector leaders can advance the security of their facilities while maintaining the operational purpose of their facility.

ACKNOWLEDGMENT

I would like to thank Dr. Roxanne Everetts for her mentorship and guidance, Dr. Chen for reading my paper and input, and my wife Erin and *les trois soeurs* for their patience and support.

REFERENCES

[1] B. Ireland, "Security Risks," *EC&M Electrical Construction and Maintenance,* pp. 10-16, January 2012.

[2] C. Copeland, "Terrorism and Security Issues Facing the Water Infrastructure Sector," Congressional Research Service, Washington D.C., 2010.

[3] A. Bolshev and I. Yushkevich, "SCADA and Mobile Security in the Internet of Things Era," 6 January 2017. [Online]. Available: https://ioactive.com/pdfs/SCADA-and-Mobile-Security-in-the-IoT-Era-Embedi-FINALab%20(1).pdf. [Accessed 28 January 2018].

[4] National Institute of Standards and Technology, SP 800-37r1 Information Security: Guide for Applying the Risk Management Framework to Federal Systems, Gaithersburg: NIST, 2010.

[5] Department of Homeland Security, "National Infrastructure Protection Plan 2013," Department of Homeland Security, Washington D.C., 2013.

[6] National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity," February 2014. [Online]. Available: https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

[7] J. Hieb, J. Graham, J. Schreiver and K. Moss, "Security Preprocessor for Industrial Control Networks," in *Proceedings of the Interenational Conference on Information Warfare and Security*, 2012

[8] Congressional Budget Office, "Public Spending on Transportation and Water Infrastructure, 1956 to 2014," Congress, Washington D.C., 2015

[9] G. W. Bush, "Homeland Security Presidential Directive 7," 17 December 2003. [Online]. Available: https://www.dhs.gov/homeland-security-presidential-directive-7.

[10] W. Clinton, "Presidential Decision Directive NSC-63," 16 October 1998. [Online]. Available: https://fas.org/irp/offdocs/pdd/pdd-63.htm. [Accessed 18 February 2018].

[11] B. Obama, "Executive Order 13636 Improving Critical Infrastructure Cybersecurity," White House, Washington D.C., 2013.

[12] B. Obama, "PPD 21," White House, Washington D.C., 2013.

[13] Department of Homeland Security and Environmental Protection Agency, Water and Wastewater Sector-Specific Plan 2015, Washington D.C.: EPA, 2015.

[14] L. Van Leuven, "Water/Wastewater Infrastructure Security: Threats and Vulnerabilities," in *Handbook of Water and Wastewater Systems Protection*, Springer, 2011, pp. 27-46.

[15] Government Accountability Office, "Critical Infrastructure Protection: Multiple Efforts to Secure Systems are Underway but Challenges Remain," Government Accountability Office, Washington D.C., 2007.

[16] Department of Homeland Security, "ICS-CERT Annual Assessment Report FY2016," Department of Homeland Security, Washington D.C., 2017.

[17] Positive Technologies, "ICS Security: 2017 in Review," Positive Technologies, 2018.

[18] L. Newman, "Menacing Malware Shows the Dangers of Industrial System Sabotage," 18 January 2018. [Online]. Available: https://www.wired.com/story/triton-malware-dangers-industrial-system-sabotage/. [Accessed 20 January 2018]

[19] K. Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon," November 2014. [Online]. Available: https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/. [Accessed 20 February 2018].

[20] K. Zetter, "Iran: Computer Malware Sabotaged Uranium Centrifuges," 29 November 2010. [Online]. Available: https://www.wired.com/2010/11/stuxnet-sabotage-centrifuges/. [Accessed 20 February 2018].

[21] D. M. Birkett, "Water Critical Infrastructure and Its Dependencies," *Journal of Terrorism Research,* vol. 8, no. 2, pp. 1-21, May 2017.

[22] D. Kroll, K. King, T. Engelhardt, M. Gibson, K. Craig and Hach Homeland Security Technologies, "Terrorism Vulnerabilities to the Water Supply and the Role of the Consumer: Water Security White Paper," March 2010. [Online]. Available: http://www.waterworld.com/articles/2010/03/terrorism-vulnerabilities-to-the-water-supply-and-the-role-of-the-consumer.html. [Accessed 20 February 2018].

[23] 107th Congress, "The Public Health Security and Bioterrorism and Response Act of 2002," 12 June 2002. [Online]. Available: https://www.gpo.gov/fdsys/pkg/PLAW-107publ188/pdf/PLAW-107publ188.pdf. [Accessed 18 February 2018].

[24] T. G. Lewis, "Critical Iinfrastructure Protection in Homeland Security : Defending a Networked Nation," in *Critical Iinfrastructure Protection in Homeland Security : Defending a Networked Nation*, Palo Alto, John Wiley & Sons, 2015, pp. 185-203.

[25] M. Lewis, "Cross-connection and Backflow Devices," January 2011. [Online]. Available: https://www.wvdhhr.org/oehs/eed/swap/training&certification/cross-connection&backflow/documents/Cross_Connection_Backflow_Prevention.pdf. [Accessed 20 March 2018].

[26] S. Jerome, "Federal Officials Warn Rural Water Systems Of Cyber Threats," 17 March 2017. [Online]. Available: https://www.wateronline.com/doc/federal-officials-warn-rural-water-systems-of-cyber-threats-0001. [Accessed 3 March 2018].

[27] B. Rios and T. McCorkle, "McCorkle and Rios: 100 bugs in 100 days," 7 October 2011. [Online]. Available: https://www.youtube.com/watch?v=29S_Beg71dA. [Accessed 17 February 2018].

[28] R. McMillan, "Hackers break into water system network," 1 November 2006. [Online]. Available: https://www.infoworld.com/article/2659670/security/hackers-break-into-water-system-network.html. [Accessed 3 March 2018].

[29] M. Abrams and J. Weiss, "Malicious Control System Cyber Security Attack Case Study-Maroochy Water Services Case Study," 28 July 2008. [Online]. Available: https://www.mitre.org/sites/default/files/pdf/08_1145.pdf. [Accessed 30 January 2018].

[30] R. A. Clark and R. A. Deninger, "Protecting the Nation's Critical Infrastructure:," *Journal of Contingencies and Crisis Management,* vol. 8, no. 2, pp. 73-80, 2000.

[31] Government Accountablity Office, "Securing Wastewater Facilities: Costs of Risk Assessments, Risk Management Plans, and Alternative Disinfection Methods Vary Widely," March 2007. [Online]. Available: https://www.gao.gov/assets/260/258480.pdf. [Accessed 2 February 2018].

[32] Government Accountability Office, "Critical Infrastructure Protection: Additional Actions Are Essential for Assessing Cybersecurity Framework Adoption," Government Accountability Office, Washington D.C., 2018.

[33] P. Pederson, D. Dudenhoffer, S. Hartley and M. Permann, "Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research," Idaho National Laboratory, Idaho Falls, 2006.

[34] P. Valentia, *Water Sector Cyber Threat Briefing,* 2018.

[35] American Water Works Association, "Process Control System Security Guidance for the Water Sector," AWWA, 2017.

[36] E. G. Bachman, "Pre-planning for Emergencies at Water Treatment Facilities," *Fire Engineering,* vol. 156, no. 8, pp. 120-130, August 2003.

[37] WaterISAC, "10 Basic Cybersecurity Measures," June 2015. [Online]. Available: https://ics-cert.us-cert.gov/sites/default/files/documents/10_Basic_Cybersecurity_Measures-WaterISAC_June2015_S508C.pdf. [Accessed 24 February 2018].

[38] D. Verner, F. Petit and K. Kim, "Prioritization in Critical Infrastructure," *Homeland Security Affairs,* vol. 13, October 2017.

[39] National Institute of Standards and Technology, "SP 800-39 Managing Information Security Risk: Organization, Mission, and Information System View," March 2011. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-39/final.

[40] DOD, "DODI 8510.01 DIACAP," November 2007. [Online]. Available: http://www.dtic.mil/dtic/tr/fulltext/u2/a551538.pdf.

[41] Department of Homeland Security, "NCCIC ICS-CERT Assessments FAQ," May 2016. [Online]. Available: https://ics-cert.us-cert.gov/sites/default/files/documents/NCCIC%20ICS-CERT%20Assessment%20FAQ_S508C.pdf. [Accessed 23 February 2018].

[42] Environmental Protection Agency, "Conduct a Water or Wastewater Utility Risk Assessment," EPA.gov, 12 October 2017. [Online]. Available: https://www.epa.gov/waterriskassessment/conduct-drinking-

water-or-wastewater-utility-risk-assessment. [Accessed 19 February 2018].

[43] M. McWhirt, "August 20, 2014 Cybersecurity Assessments and Tools DHS," 20 August 2014. [Online]. Available: https://www.waterisac.org/portal/august-20-2014-cybersecurity-assessments-and-tools-dhs. [Accessed 23 February 2018].

[44] Environmental Protection Agency. (2017, October 26). *VSAT 6.0*. Retrieved July 2, 2018, from EPA.gov: https://vsat.epa.gov/vsat/

[45] K. Dillon, "Cybersecurity Assessments and Tools by DHS," 20 August 2014. [Online]. Available: https://www.waterisac.org/portal/august-20-2014-cybersecurity-assessments-and-tools-dhs. [Accessed 23 February 2018].

[46] WaterISAC, "About Us," 2017. [Online]. Available: https://www.waterisac.org/about-us. [Accessed 5 March 2018].

[47] Environmental Protection Agency, "Learning from State Water Emergency Response Exercises," May 2012. [Online]. Available: https://www.epa.gov/waterresiliencetraining/learn-state-water-emergency-response-exercises. [Accessed 2 February 2018].

[48] Government Accountability Office, "Wastewater Facilities: Experts' Views on How Federal Funds Should Be Spent to Improve Security," GAO, Washington D.C., 2005.

[49] Environmental Protection Agency, "National Primary Drinking Water Regulations," 21 August 2016. [Online]. Available: https://www.epa.gov/sites/production/files/2016-06/documents/npwdr_complete_table.pdf. [Accessed 18 February 2018].

[50] J. Schriever, *Role based access control and authentication for SCADA field devices using a dual Bloom filter and challenge response,* 1281 ed., Kentucky: University of Louisville, 2012.

[51] National Institute of Standards, "Guide to Industrial Control System (ICS) Security," May 2015. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final. [Accessed 24 February 2018].

[52] Environmental Protection Agency, “WSI Pilot Summary Report,” October 2015. [Online]. Available: https://www.epa.gov/sites/production/files/2015-12/documents/wsi_pilot_summary_report_102715.pdf. [Accessed 4 September 2018]