Critical Infrastructure Security and Resilience Note: Cyber-Physical Vulnerability and Consequence Considerations for the Water and Wastewater Systems Sector

September 25, 2014, 0930 EDT

SCOPE

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 to provide increased awareness of related threats, vulnerabilities, and consequences. This report contains vulnerability, consequence, and mitigation findings based on a series of cyber-physical site assessments that an OCIA-led team conducted over the last year with several public and private sector partners. Groundwork for the assessments began in the summer of 2012, launching a substantial effort that involved collaboration with the National Protection and Programs Directorate Office of Infrastructure Protection/Protective Security Coordination Division and Office of Cybersecurity and Communications/Industrial Control Systems Computer Emergency Response Team (ICS-CERT); Idaho National Laboratory; and Los Alamos National Laboratory.

This report does not include specific information captured during the site assessments, such as the names and locations of the facilities. In addition, this report does not address specific threat actors or extensive details of the attack techniques they could employ to exploit identified vulnerabilities. The report does characterize possible impacts and consequences that could potentially result from cyber-based penetrations within a variety of water and wastewater systems.

This report seeks to build on—not duplicate—previous materials that Water and Wastewater Systems Sector stakeholders have developed, including the "Roadmap to Secure Control Systems in the Water Sector."[2] In addition, OCIA recognizes that the limited number of sites involved in the series of cyber-physical site assessments do not—and cannot—represent the numerous possible ICS implementations that exist in other Water and Wastewater Systems Sector utilities. OCIA developed this report to provide overarching, rather than site-specific considerations, which are intended to support Water and Wastewater Systems Sector utilities; share the significance of assessing potential vulnerabilities and consequences to better

[1] In February 2014, the DHS National Protection and Programs Directorate (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] Water Sector Coordinating Council Cyber Security Working Group, "Roadmap to Secure Control Systems in the Water Sector," March 2008, www.awwa.org/portals/0/files/legreg/security/securityroadmap.pdf, accessed May 1, 2014.

understand potential risks; provide considerations for enhancing cybersecurity posture and resilience; and inform risk-management decisions.[3]

KEY FINDINGS

- **The OCIA-led team assessed two key vulnerabilities that present possible Internet-based vectors for attackers to gain unauthorized access to Water and Wastewater Systems Sector systems:**
  - **Blending industrial control systems (ICS) and business networks within an operations center rather than keeping them isolated and segmented.**
  - **Running Web services on an ICS-connected device to support Internet-based remote monitoring of ICS operations.**
- **An attacker that gains unauthorized access via the Internet or a trusted connection—such as a third-party vendor—can potentially exploit ICS vulnerabilities to maliciously operate disinfectant pumps or valves, cripple the supervisory control and data acquisition (SCADA) system, or steal data.**
- **Water utility supply, treatment, and transmission components with local control capabilities can allow staff to operate manually while isolating distributed control system or SCADA components, which reduces the potential for consequences.**

OVERVIEW

As water utilities expand their reliance upon information technology and begin integrating ICS infrastructure to increase productivity and reduce operating costs, such reliance exposes utilities to potential cyber-related risks. Since the summer of 2013, OCIA has partnered with several water treatment plants to conduct a variety of in-depth, cyber-physical site assessments. For each assessment, OCIA worked with national laboratory partners to identify site-specific cybersecurity vulnerabilities and then used hydraulic modeling and simulation to assess the potential physical consequences of a threat actor exploiting the site-specific vulnerabilities. OCIA provided each site with a cyber-physical site assessment report, which included mitigation suggestions using ICS-CERT best practices to assist the site with enhancing its cybersecurity posture and resilience.

[3] In August 2014, OCIA released a Critical Infrastructure Security and Resilience Note: "Water and Wastewater Systems Sector Cyberdependencies," which is intended to inform 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. The document also clarifies how computer systems support infrastructure operations, how cybersecurity incidents may or may not compromise these operations, and the likely functional outcome of these compromises. In addition, ICS-CERT provides alerts and advisories (among other products and services) to notify critical infrastructure owners and operators about current security issues, including threats to asset networks, vulnerabilities, and exploits. For more information, visit: https://ics-cert.us-cert.gov/.

Water and Wastewater Systems Sector infrastructure throughout the United States can be the target of threats that originate from a variety of international and domestic sources, including adversarial governments, criminal groups, terrorists, disgruntled employees, and hackers. DHS has provided guidance to help utilities develop defense-in-depth strategies to thwart cybersecurity threats.[4]

VULNERABILITIES AND MITIGATION OPTIONS

While conducting the series of cyber-physical site assessments, the OCIA-led team observed an operations center using blended ICS and business networks that were directly interconnected instead of segregated, allowing communication flows to traverse from one network to another. In addition, the team observed staff remotely accessing a Web server from outside the network perimeter to obtain real-time information on a water system. Running Web services on an ICS-connected device to support monitoring ICS operations from a remote location introduces another potential attack vector that a threat actor can exploit. Although the staff identified the Web server and SCADA software as running on two separate devices in a network diagram, the OCIA-led team discovered they were physically running on the same server. In addition, this particular case potentially poses an availability issue for both services if the server became inoperable. Reviewing the logical and physical configurations to confirm separation is a way to avoid the vulnerabilities that such overlap exposes.

Keeping ICS and business network operations separate is a key mitigation option that the team shared with multiple facilities based on site findings. For example, to reduce the likelihood that a threat actor could potentially exploit trusted connections between systems within non-ICS network segments and downstream systems within the control systems environment, the team advised that water utilities install a demilitarized zone, which could prevent a business node from directly accessing the control system network (and vice versa) if properly configured.[5]

In addition, the team recommended other ICS-CERT best practices, including that each site should establish a security zone—a dedicated and secured network segment that houses security-centric devices while remaining isolated from the corporate control system—and include tools that monitor and maintain the security posture of ICS implementations.

In a separate instance, the OCIA-led team observed a different overlap of ICS and business networks. A utility configured an Active Directory on its business network to authenticate and authorize users on the control systems network. The configuration posed a potential problem because it directly established a trusted relationship between the business and control system networks. If a threat actor were able to gain unauthorized access to the business network, the actor could then exploit that access and the trusted relationship to authenticate and authorize the actor's access to the control systems network. To mitigate the vulnerability, the team recommended that the utility implement a dedicated Active Directory domain instance for the control system network to uniquely authenticate control system networks users.

[4] DHS Control Systems Security Program, "Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies," October 2009, http://ics-cert.us-cert.gov/sites/default/files/recommended_practices/Defense_in_Depth_Oct09.pdf, accessed April 28, 2014.

[5] For more information about demilitarized zones, see p. 7 of DHS, ICS-CERT, "ICS-CERT Monitor," January–April 2014, http://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_%20Jan-April2014.pdf, accessed June 9, 2014.

The National Institute of Standards and Technology recommends mitigation options that include a defense-in-depth approach to securing Water and Wastewater Systems Sector ICS. This approach recognizes that a singular security product or technological approach is unable to adequately protect an ICS. Instead, a defense-in-depth approach provides a multilayer strategy in which overlapping security mechanisms reduce the overall impact to the system if one mechanism fails. The recommended strategy includes using firewalls, demilitarized zones, intrusion detection capabilities (along with other aspects of detection and monitoring capabilities), effective security policies, training programs, and incident response mechanisms.[6]

POTENTIAL CONSEQUENCES

If a defense-in-depth approach can reduce the potential consequences stemming from one system failure, then that approach contributes to the resilience of the system. Resilience is realized in other ways, as well. For example, the Water and Wastewater Systems Sector utilities that OCIA assessed have a relatively unique resilience posture due to the proximity of the utility systems to each other. OCIA found that each system has multiple sources of normal or emergency water supply via interconnections.

In addition to, or in the absence of, such interconnections, many Water and Wastewater Systems Sector utilities employ standard operating procedures (e.g., locking ICS components in enclosures, taking water quality samples routinely, and inspecting anomalies visually when they appear through data monitoring). Although standard operating procedures can help to reduce the potential for significant consequences from a cyber attack, threat actors may still find opportunities to exploit water utilities' connectivity between cyber and physical systems in ways that result in consequences.

For instance, OCIA found that, depending on how a utility configures its ICS operations, a cyber attack on a re-chlorination facility could create two potential physical consequences:

- An excess dose of sodium hypochlorite (albeit of a minimal amount) that results in customers reporting a chlorine smell to the water utility.
- No disinfectant boost being added to the water distribution system, possibly resulting in gastrointestinal problems for people with compromised immune systems.[7]

In addition, OCIA assessed that damage to critical components, such as pumps, could result in water utilities bypassing treatment processes, requiring the issuance of boil water notices to customers. These consequences illustrate how downstream customers may be affected if a cyber attack successfully disrupts a water utility.

Cyber attacks can potentially lead to internal consequences, as well. For example, if a threat actor were able to spoof or change real-time data within a SCADA system, OCIA assessed that such attacks could lead to erroneous operational decisions or a partial or total loss of the SCADA. The loss of SCADA systems could prompt staff to revert to manual operations, which could inhibit the water utility's ability to efficiently run and monitor operations.

[6] National Institute of Standards and Technology, "Guide to Industrial Control Systems (ICS) Security," Special Publication 800-82, June 2011, pgs. 5–10, http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf, accessed May 22, 2014.

[7] Based on analysis that Los Alamos National Laboratory developed to support the cyber-physical site assessments that OCIA conducted in the summer of 2013.

Practicing standard operating procedures to identify potential problems with operations or the treatment process can help limit the potential consequences of disruptions. More broadly, a water utility may be resilient to short-term water supply disruptions if the utility's reservoir has a large enough volume of stored, treated water.

In general, OCIA found that the capability for staff to operate water utility infrastructure manually, especially while isolating distributed control system or SCADA components, mitigates the potential for significant consequences. In one instance, the water treatment plant design allowed manual operation of the entire plant; operators could use local control at the pumps to lock out the SCADA system if a threat actor gained control of the SCADA to operate pumps. However, the utility would need a mechanism in place to detect that the intrusion had occurred.

CONCLUSION

Overall, OCIA assessed that disruptions to water treatment plants can have physical consequences at the utilities in addition to downstream impacts for customers.[8] Employing sound cybersecurity practices can make it more challenging for threat actors to create disruptions. At the same time, cybersecurity measures for Water and Wastewater Systems Sector utilities are not currently regulated, nor are there mandatory reporting requirements in the event that a water utility is the target of a cyber attack.

In place of specific regulations, the Water and Wastewater Systems Sector has focused efforts on recognizing the potential vulnerability concerns related to ICS networks and cybersecurity, as well as using other mechanisms to enhance their overall resilience. Understanding these vulnerabilities is a starting point that utilities can use to establish more robust cybersecurity postures.

The cyber-physical site assessments conducted by OCIA do more than just highlight cybersecurity concerns. The assessments also added focus on specific potential physical consequences of a threat actor exploiting site-specific vulnerabilities. Utilities that consider potential physical consequences of disruptions and exploited vulnerabilities are more informed and better positioned to prioritize fixing vulnerabilities based on the severity of the consequences.

The Office of Cyber and Infrastructure Analysis (OCIA) produces Critical Infrastructure Security and Resilience Notes that address emerging risks to critical infrastructure and provide increased awareness of the implications of those risks to the Homeland. The information is provided to support the activities of DHS, and to inform the strategies and capabilities of Federal, State, local, and private sector partners. For more information, contact OCIA@hq.dhs.gov or visit our Website: www.dhs.gov/office-cyber-infrastructure-analysis.

[8] Other sources contain additional consequence considerations. For example, see the section titled "How Can Cyber Attacks Affect Water Systems?" in the U.S. Environmental Protection Agency's, "Cyber Security101 for Water Utilities," July 2012, http://water.epa.gov/infrastructure/watersecurity/features/upload/epa817k12004.pdf, accessed May 21, 2014.