OFFICE of INTELLIGENCE and ANALYSIS
INTELLIGENCE IN FOCUS
20 MAY 2021 IA-49495-21

CYBERSECURITY

(U) Malicious Cyber Actors Likely to Continue Exploiting Vulnerabilities in Water and Wastewater Systems Networks

(U) ***We assess that high profile cyber attacks against water and wastewater systems (WWS) sector networks will increase as criminal, nation-state, and terrorist cyber actors seek to exploit enduring vulnerabilities to achieve financial, geopolitical, or ideological objectives.*** We base this assessment on successful cyber actor targeting since at least 2018—and as recent as February 2021—of US and foreign WWS sector networks. Malicious cyber activity against US and international water facilities is common and typically undertaken to secure ransom payments, highlight political or social causes, or the sector is targeted in the context of a broader geopolitical issue or conflict.

- (U) On 5 February 2021, unidentified cyber actors exploited unsecured remote access software to gain unauthorized access to the industrial control system (ICS) at a US drinking water treatment plant in Oldsmar, Florida, according to a joint governmental cybersecurity advisory. Once on the network, the unidentified cyber actors had full access to the plant's virtual human machine interface (HMI) and used that access to increase the amount of sodium hydroxide—also known as lye, a caustic chemical—in the water treatment process. Water treatment plant personnel noticed the change in dosing amounts and corrected the issue before the ICS software detected the manipulation and shut down the system due to unsafe conditions, according to the same cybersecurity advisory.

- (U) An unidentified cyber actor in October 2018 infected the Onslow Water and Sewer Authority[USPER] in Jacksonville, North Carolina with Ryuk ransomware, according to media reporting. The Onslow facility serves approximately 150,000 people. The attack forced the facility to perform many previously automated processes manually, which greatly degraded the timeliness and efficiency of the facility for weeks following the attack. The facility opted to not pay the ransom, requiring a complete rebuild of databases and systems to restore access, according to the same media reporting.

- (U) Geopolitical tensions between Iran and Israel have led to Iranian cyber attacks against the Israeli water sector, according to a reliable media report. Possible Iran-linked cyber actors in April 2020 attempted to disrupt operations at two Israeli water facilities by targeting ICS controllers that operated valves in water distribution systems. The intrusions were caught before they could impact the water supply, according to the same media report.

(U) Prepared by the Cyber and Counterterrorism Mission Centers. Coordinated within the DHS Intelligence Enterprise (CETC, CISA, CWMD, FOD, ICE, TSA, USCG) and with EPA. For questions, contact DHS-SPS-RFI@hq.dhs.gov

- *(U)* International terrorist groups have also demonstrated interest in targeting the WWS sector through both physical and cyber-enabled methods. In June 2018, a Wisconsin-based Islamic State of Iraq and ash-Sham (ISIS) supporter used a pro-ISIS social media account to encourage a suspected ISIS supporter to poison water reservoirs with ricin—presumably not via cyber means—according to a Department of Justice (DOJ) press release. In addition, the June 2020 issue of al-Qa'ida's English-language magazine, *One Ummah*, encouraged compromising critical infrastructure, including water systems, and asked followers to develop cyber warfare capabilities on their own or in small groups to launch cyber attacks, according to a Western media report.

(U) **Complexity of Industrial Control System in the Water and Wastewater Systems Sector Presents Challenges to Destructive Cyber Attacks**

(U) ICS in the WWS sector includes multiple process controllers, HMIs, diagnostics, and automated safety instrumented systems (SIS) on critical processes, according to a NIST publication on ICS security. As information technology (IT) and ICS converge—the seam between cyberspace and the physical world—and internet pathways to ICS increase, cyber actors gain new attack vectors, especially as ICS device cybersecurity lags IT, according to an academic research paper submitted to a cybersecurity conference. Still, despite these new vulnerabilities, a cyber actor seeking to inflict physical harm on the public must gain control over multiple key components of the targeted WWS sector's ICS. This complexity, along with human operator oversight, presents inherent challenges to a threat actor.

(U) For a cyber attack to work most effectively, an actor would need to access key control systems, set operating parameters beyond safe limits, disable or manipulate SIS to hamper detection and sustain unsafe conditions, and also prevent operator interference, according to a NIST publication on ICS security. This type of operation requires extensive *undetected* lateral movement across the ICS network and could also require multiple device-specific malware tools and familiarity with the hardware and software configuration. While remediating the events discussed in this assessment cost time and money, individual plant processes and a human-in-the-loop element greatly decreased the chance of harm to the public. In the February 2021 Florida drinking water treatment plant compromise, the cyber actor—who was almost immediately detected—had access to the process controller but had not disabled the SIS or locked the HMI, which allowed a technician to reset the system to safe parameters.

(U) ***We are unaware of any terrorist-affiliated cyber actor with a sophisticated offensive cyber attack capability—unlike nation-state and organized cybercriminals—although terrorist actors, including groups supporting or affiliated with ISIS and al-Qa'ida, likely will continue to seek to develop more advanced cyber capabilities to compromise critical infrastructure.*** We base this assessment on nation-state, terrorist, and criminal cyber actor activity between August 2013 and November 2020, which revealed uneven cyber capabilities amongst the threat actors. We have no information suggesting a successful compromise of, or imminent threat to, the

cybersecurity of the US WWS sector by terrorist actors. The relatively limited number of cyber attacks by terrorist actors indicates that an attack on the WWS sector is likely more aspirational in nature at the present time. However, the relatively basic technical skill required to achieve the February 2021 Florida drinking water treatment plant compromise suggests that even amateur cyber actors could conduct a similar attack at small WWS sector facilities with limited cybersecurity resources.

- *(U)* Pro-ISIS and pro-al-Qa'ida cyber actors have conducted a limited range of cyber activities on behalf of the respective groups, focusing primarily on website defacement; denial-of-service (DoS); collecting personally identifiable information (PII) of US Government personnel, including for the purpose of building "kill lists"; and spreading propaganda for intimidation and recruitment, according to Western media reporting and an online independent journal. Cyber tools and guides are readily available online, which terrorist organizations, affiliated groups, and sympathizers can use to acquire the necessary skills to conduct more advanced cyber operations. However, we currently lack evidence of a more sophisticated capability.
- *(U)* An anti-Israeli cyber group in 2020 conducted a series of cyber attacks targeting Israeli wastewater facilities and other critical infrastructure, according to a cybersecurity firm report. Though we have not seen cyber attacks that approximate this level of sophistication in the United States, cyber tools and guides available on the deep and dark web offer relatively accessible training resources for individuals interested in developing these cyber skills, according to Western media reporting.

(U) Analysis of Alternatives

(U) Two alternatives could alter the threat equation when considering the ability to detect cyber intrusions, pace and accuracy of attribution, and assessments of threat actor capabilities.

- *(U)* First, it is possible that other WWS sector entities have been compromised and cyber actors maintain undetected persistent access to WWS sector networks. Many WWS entities do not have robust cybersecurity, and recent cyber activity such as the SolarWinds[USPER] supply chain attack demonstrates the ability of highly skilled cyber actors to gain and maintain network accesses; similar operations may continue undetected. We rejected the possibility that nation-state cyber actors would—absent a conflict with the United States—exploit this access to cause physical destruction or public harm, due to almost certain backlash and reprisal.
- *(U)* Second, it is possible that we have misjudged the current capabilities of non-state cyber actors, and that terrorists and cybercriminals possess a greater capability to attack the WWS sector than assessed. Positive attribution of a physically destructive cyber attack on the ICS devices of a WWS entity to a terrorist-affiliated cyber actor would significantly alter our assessment.

(U) Mitigation Resources

(U) **The FBI, Cybersecurity and Infrastructure Security Agency (CISA), Environmental Protection Agency (EPA), and Multi-State Information Sharing and Analysis Center (MS-ISAC) have released a joint cybersecurity advisory detailing steps WWS sector entities should take to mitigate risk of future attacks.**[a] These recommendations include general cybersecurity best practices, as well as specific guidance for WWS sector security and use of remote control software. Additionally, the NSA and CISA released a cybersecurity advisory recommending actions that operational technology (OT) network operators across all critical infrastructure sectors should immediately adopt to secure their OT systems.[b] Additionally, the websites of the MS-ISAC, Water ISAC, and the US Computer Emergency Readiness Team (US-CERT) websites contain alerts, advisories, best practices, and other valuable data for protecting OT assets against cyber threats.

[a] *(U)* This *Advisory* is available at: https://us-cert.cisa.gov/sites/default/files/publications/AA21-042A_Joint_Cybersecurity_Advisory_Compromise_of_U.S._Drinking_Treatment_Facility.pdf.
[b] *(U)* This *Advisory* is available at: https://media.defense.gov/2020/Jul/23/2002462846/-1/-1/1/OT_ADVISORY-DUAL-OFFICIAL-20200722.PDF.

Source, Reference, and Dissemination Information

Source Summary Statement	(U) We assess that criminal, nation-state, and terrorist cyber actors likely will continue to seek opportunities to compromise networks in the WWS sector, exploiting enduring network vulnerabilities in the sector to achieve geopolitical, ideological, or financial objectives. We have **medium confidence** in our assessment, based on reliable Western media reporting, a joint governmental cybersecurity advisory, and a report from a reputable cybersecurity firm. Additional reporting on continued attempts by nation-state, terrorist, and criminal cyber actors to exploit WWS sector cybersecurity vulnerabilities likely would increase our confidence in this assessment. (U) We are unaware of any terrorist-affiliated cyber actor with a sophisticated offensive cyber attack capability—unlike nation-state and organized cybercriminals—although terrorist actors, including groups supporting or affiliated with ISIS and al-Qa'ida, likely will continue to seek to develop more advanced cyber capabilities to compromise critical infrastructure. We have **medium confidence** in our assessment based on reliable Western media reporting, DOJ press releases, reputable cybersecurity firm reports, and an online independent journal. Additional reporting on cyber threat actors' capability to exploit WWS sector cybersecurity vulnerabilities likely would increase our confidence in this assessment.
Definitions	(U) **Denial-of-Service (DoS):** A type of cyber attack designed to prevent users from accessing a network-connected service by sending illegitimate requests from one source. Data is sent to overload a network's resources. (U) **Industrial Control Systems (ICS):** A computer or network that controls physical processes for industrial facilities and infrastructures.
Reporting Suspicious Activity	(U) **To report suspicious activity, law enforcement, Fire-EMS, private security personnel, and emergency managers should follow established protocols; all other personnel should call 911 or contact local law enforcement.** Suspicious activity reports (SARs) will be forwarded to the appropriate fusion center and FBI Joint Terrorism Task Force for further action. For more information on the Nationwide SAR Initiative, visit http://nsi.ncirc.gov/resources.aspx. (U) **To report a computer security incident, either contact US-CERT at 888-282-0870, or go to https://forms.us- cert.gov/report/ and complete the US-CERT Incident Reporting System form.** The US-CERT Incident Reporting System provides a secure, web-enabled means of reporting computer security incidents to US-CERT. An incident is defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. In general, types of activity commonly recognized as violating typical security policies include attempts (either failed or successful) to gain unauthorized access to a system or its data, including personally identifiable information; unwanted disruption or denial of service; the unauthorized use of a system for processing or storing data; and changes to system hardware, firmware, or software without the owner's knowledge, instruction, or consent.
Dissemination	(U) Federal, state, local, tribal, territorial, and private sector network defenders.
Warning Notices & Handling Caveats	(U) **Warning**: This document is UNCLASSIFIED (U). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to Unclassified information and is not to be released to the public, the media, or other personnel who do not have a valid need to know without prior approval of an authorized DHS official. State and local homeland security officials may share this document with authorized critical infrastructure and

	key resource personnel and private sector security officials without further approval from DHS. *(U)* This product contains US person information that has been deemed necessary for the intended recipient to understand, assess, or act on the information provided. It has been highlighted in this document with the label USPER and should be handled in accordance with the recipient's intelligence oversight and/or information handling procedures. Other US person information has been minimized. Should you require the minimized US person information on weekends or after normal weekday hours during exigent and time sensitive circumstances, contact the Current and Emerging Threat Watch Office at 202-447-3688, CETC.OSCO@hq.dhs.gov. For all other inquiries, please contact the Homeland Security Single Point of Service, Request for Information Office at DHS-SPS-RFI@hq.dhs.gov, DHS-SPS-RFI@dhs.sgov.gov, DHS-SPS-RFI@dhs.ic.gov.

CLASSIFICATION:

Homeland Security

Office of Intelligence and Analysis
Customer Feedback Form

Product Title: (U) Malicious Cyber Actors Likely to Continue Exploiting Vulnerabilities in Water and Wastewater Systems N

All survey responses are completely anonymous. No personally identifiable information is captured unless you voluntarily offer personal or contact information in any of the comment fields. Additionally, your responses are combined with those of many others and summarized in a report to further protect your anonymity.

1. Please select partner type: Select One **and function:** Select One

2. What is the highest level of intelligence information that you receive? Select One

3. Please complete the following sentence: "I focus most of my time on:" Select One

4. Please rate your satisfaction with each of the following:

	Very Satisfied	Somewhat Satisfied	Neither Satisfied nor Dissatisfied	Somewhat Dissatisfied	Very Dissatisfied	N/A
Product's overall usefulness	○	○	○	○	○	○
Product's relevance to your mission	○	○	○	○	○	○
Product's timeliness	○	○	○	○	○	○
Product's responsiveness to your intelligence needs	○	○	○	○	○	○

5. How do you plan to use this product in support of your mission? ***(Check all that apply.)***

- ☐ Drive planning and preparedness efforts, training, and/or emergency response operations
- ☐ Observe, identify, and/or disrupt threats
- ☐ Share with partners
- ☐ Allocate resources (e.g. equipment and personnel)
- ☐ Reprioritize organizational focus
- ☐ Author or adjust policies and guidelines
- ☐ Initiate a law enforcement investigation
- ☐ Intiate your own regional-specific analysis
- ☐ Intiate your own topic-specific analysis
- ☐ Develop long-term homeland security strategies
- ☐ Do not plan to use
- ☐ Other:

6. To further understand your response to question #5, please provide specific details about situations in which you might use this product.

7. What did this product *not* address that you anticipated it would?

8. To what extent do you agree with the following two statements?

	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disgree	N/A
This product will enable me to make better decisions regarding this topic.	○	○	○	○	○	○
This product provided me with intelligence information I did not find elsewhere.	○	○	○	○	○	○

9. How did you obtain this product? Select One

10. Would you be willing to participate in a follow-up conversation about your feedback? Yes

To help us understand more about your organization so we can better tailor future products, please provide:

Name:		*Position:*	
Organization:		*State:*	
Contact Number:		*Email:*	

Submit Feedback

Privacy Act Statement

CLASSIFICATION:

Product Serial Number: REV: 01 August 2017