hackerone

September 14, 2025

New York State Department of Health
Bureau of Program Counsel, Regulatory Affairs Unit
Empire State Plaza Albany, New York 12237

VIA ELECTRONIC SUBMISSION

Re: Cybersecurity Requirements for Public Water Systems

Dear Ms. Katherine Ceroalo,

HackerOne, Inc. (HackerOne) submits the following comments in response to the New York State Department of Health (DOH)'s proposed additions under 10 NYCRR Part 5, Subpart 5-1 of the New York Codes, Rules, and Regulations, referred to as the "Public Water System Cybersecurity Rules."[1] HackerOne appreciates the opportunity to provide input and commends the DOH for advancing cybersecurity protections for public water systems.

By way of background, HackerOne is a global leader in offensive security solutions. Our HackerOne Platform combines AI with the ingenuity of the largest community of security researchers to find and fix security, privacy, and AI vulnerabilities across the software development lifecycle. The platform offers bug bounty, vulnerability disclosure, pentesting, AI red teaming, and code security. We are trusted by industry leaders like Amazon, Anthropic, Crypto.com, General Motors, GitHub, Goldman Sachs, Uber, and the U.S. Department of Defense.

While HackerOne broadly supports the Department's efforts to strengthen cybersecurity in the water sector, we believe that the following recommendations would further enhance the overall effectiveness of the proposed rules.

1. Avoid Premature Disclosure of Unmitigated Vulnerabilities.

According to the proposed rulemaking, community water systems that serve more than 3,300 people will be required to "report vulnerabilities that may impact or limit a covered water system's ability to comply with the requirements of 10 NYCRR Part 5 Subpart 5-1 to the Department of Health within 48 hours of identification."[2] While timely reporting is important, mandatory early disclosure of unmitigated vulnerabilities can create significant security and

[1] New York State Department of Health, Appendix 5-E: Cybersecurity Requirements for Public Water Systems, 10 N.Y.C.R.R. § 5-1. https://regs.health.ny.gov/sites/default/files/proposed-regulations/Cybersecurity%20Requirements%20for%20Public%20Water%20Systems.pdf.
[2] *Id.* subpart 5-E, https://regs.health.ny.gov/sites/default/files/proposed-regulations/Cybersecurity%20Requirements%20for%20Public%20Water%20Systems.pdf.

operational risks. Sharing vulnerabilities before they are assessed and mitigated provides attackers with actionable information, increasing the likelihood of exploitation and targeted attacks. Centralizing such reports could further concentrate risk, making New York systems more attractive targets.

Although the proposed rulemaking does not provide additional specifics about the nature of the required disclosure, such as the level of technical detail, reporting channels, or protections for sensitive information, even limited disclosure can carry significant risks. According to CERT, "mere knowledge of a vulnerability's existence in a feature of some product is sufficient for a skillful person to discover it for themselves."[3] Premature reporting could inadvertently reveal exploitable weaknesses in operational technology, control systems, or other critical infrastructure components before remediation occurs.

HackerOne recommends that reporting obligations be limited to vulnerabilities that have been assessed and mitigated, ensuring unmitigated vulnerabilities are not shared prematurely while still providing regulators with sufficient information for oversight and risk management.

2. Lengthen Incident Reporting Timelines

Additionally, under the proposed rules, "covered water systems are required to report cybersecurity incidents to the Department of Health within 24 hours."[4] Similar to our feedback to the New York State Department of Environmental Conservation (DEC)'s proposed rules, HackerOne is concerned that this compressed timeframe may hinder effective incident response and increase the risk of incomplete or inaccurate reporting. In the first 24 hours following an incident, response teams often lack the necessary information to fully assess scope, impact, and mitigation measures. Reporting too early could result in preliminary submissions that later require correction, potentially confusing regulators and complicating decision-making.

HackerOne recommends extending the reporting window to 72 hours. This timeline provides an appropriate balance between urgency and accuracy, allowing water systems to conduct an initial assessment, determine impact, and provide regulators with a meaningful and actionable report. A 72-hour requirement would also align with established cybersecurity reporting standards, including the New York State Department of Financial Services Cybersecurity Requirements for Financial Services Companies[5], the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA)[6], and the EU General Data Protection Regulation (GDPR)[7] – all of which adopt 72-hour reporting periods.

---

[3] CERT, Guide to Coordinated Vulnerability Disclosure, 5.7 Disclosure Timing, Sep. 16, 2019, https://vuls.cert.org/confluence/display/CVD/5.7+Disclosure+Timing#id-5.7DisclosureTiming-ReleasingPartialInf.
[4] New York State Department of Health, Cybersecurity Requirements for Public Water Systems, Section 5-E.9
[5] New York State Division of Financial Services Cybersecurity Requirements for Financial Services Companies, https://www.dfs.ny.gov/system/files/documents/2023/12/rf23_nycrr_part_500_amend02_20231101.pdf
[6] 6 U.S. Code § 681b, https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title6-section681&num=0&edition=prelim
[7] European Union (EU), General Data Protection Regulation (GDPR), Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, Article 33.

Additionally, HackerOne recommends that the incident reporting requirement take effect no sooner than one year after the rule's adoption, giving water systems sufficient time to implement internal processes, establish reporting protocols, and allocate necessary resources.

* * *

HackerOne appreciates the opportunity to provide comments on this proposed rule. We look forward to continued engagement with policymakers on these issues and are happy to discuss our response at any time.

Respectfully Submitted,

Ilona Cohen
Chief Legal and Policy Officer
HackerOne