HACKING POLICY COUNCIL

Comments to New York State Department of Health on Proposed Cybersecurity Requirements for Public Water Systems

September 15, 2025

New York State Department of Health
Corning Tower
Empire State Plaza,
Albany, NY 12237
ATTN: Katherine Ceroalo

The Hacking Policy Council ("HPC") submits the following comments in response to New York State Department of Health's proposed rule on cybersecurity requirements for public water systems.[1] The HPC is a group of industry experts dedicated to creating a more favorable legal, policy, and business environment for security vulnerability disclosure and management, good faith security research, penetration testing, bug bounty programs, and independent repair for security.[2]

With this perspective, we recognize the importance of cybersecurity for public water systems and are broadly supportive of the Department of Health's efforts to update sector security practices. We respectfully offer the following recommendations, which we believe would further strengthen the proposed rules:

1. Extend the cyber incident reporting deadline to 72 hours.
2. Incorporate vulnerability disclosure processes.

Extend the Cyber Incident Reporting Deadline to 72 Hours

The Department of Health's proposed regulation would require public water systems to report cybersecurity incidents to the Department within 24 hours of identification.[3] Additionally, within 48 hours of identification, covered water systems would be required to report vulnerabilities to the Department which might impact or limit their ability to comply with the applicable requirements of the State Sanitary Code.[4]

---

[1] Department of Health: Cybersecurity Requirements for Public Water Systems, *NYS Register* at 3, (July 16, 2025) https://dos.ny.gov/system/files/documents/2025/07/071625.pdf
[2] Hacking Policy Council, https://hackingpolicycouncil.org.
[3] Summary of Express Terms - Cybersecurity Requirements for Public Water Systems at 12, https://regs.health.ny.gov/sites/default/files/proposed-regulations/Cybersecurity%20Requirements%20for%20Public%20Water%20Systems.pdf
[4] Ibid. at 8.

While prompt reporting is essential, such a narrow window could adversely affect the quality and accuracy of the facility's incident response. Additionally, the restrictive 24-hour timeframe for reporting cyber incidents would likely lead to rushed, incomplete, or inaccurate reporting. In the initial stages of a cyber incident, key details are often unclear, making it challenging to provide a comprehensive report within this period.

We recommend establishing a reporting timeline of no less than 72 hours. A 72-hour reporting timeframe aligns well with other reporting obligations, such as the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA).[5] 72 hours is a balanced deadline between promptness and practicality that allows for a more thorough initial investigation and accurate reporting. This approach reduces the likelihood of false positives, helps ensure that reports are meaningful and actionable, and allows for better coordination with law enforcement and cybersecurity agencies.

Incorporate Vulnerability Disclosure Processes

The proposed regulation lacks specific provisions to require vulnerability disclosure and handling processes (VDPs) for public water systems' cybersecurity programs. While the Department of Health's proposed rule would require covered public water systems complete a cybersecurity vulnerability analysis,[6] the lack of reference to a VDP does not align with acknowledged cybersecurity best practices, including the NIST Cybersecurity Framework.[7]

Vulnerabilities tend to be identified through a variety of sources, some of which are solicited through proactive scanning (i.e., penetration testing), while others are discovered independently from external sources. A significant volume of vulnerabilities and breaches are found by third parties, such as other vendors, service providers, security researchers, or other external sources, rather than through an organization's traditional active monitoring process. It is critical that vulnerabilities are reported, regardless of who finds them, so that they can be mitigated to protect the security of public water systems' information systems.

VDPs are foundational in modern cybersecurity frameworks. They provide organizations with a formal channel for receiving reports about vulnerabilities as they are discovered, evaluating or validating the vulnerabilities, and mitigating them. This external collaboration is invaluable for identifying vulnerabilities that internal security teams may overlook.

VDPs need not provide authorization to test systems for vulnerabilities, nor any remuneration if a vulnerability is found. In fact, vulnerabilities are routinely discovered accidentally. The purpose of the VDP is to shorten the length of time between vulnerability discovery and mitigation. Without a formal VDP, public water systems may face unaddressed security vulnerabilities for longer periods, leading to increased risks of data breaches and successful cyberattacks.

---

[5] 6 USC 681b(a).

[6] Summary of Express Terms - Cybersecurity Requirements for Public Water Systems at 7, https://regs.health.ny.gov/sites/default/files/proposed-regulations/Cybersecurity%20Requirements%20for%20Public%20Water%20Systems.pdf

[7] NIST, Framework for Improving Critical Infrastructure Cybersecurity, version 1.1, RS.AN-5, Apr. 16, 2018, at 42 https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

Consider the following language: *Each covered water system's cybersecurity program shall establish policies and procedures to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers). Such vulnerability disclosure and handling processes should be informed by standards and best practices.*[8]

We thank the New York State Department of Health for the opportunity to provide these comments and welcome continued engagement on this issue.

Sincerely,

Hacking Policy Council

[8] This language reflects NIST, Framework for Improving Critical Infrastructure Cybersecurity, version 1.1, RS.AN-5. See also ISO/IEC 29147:2018 and ISO/IEC 30111:2019.