Bond Case Briefs

Municipal Finance Law Since 1971

Fitch-Rated U.S. Water and Sewer Utilities Resilient to Cyber Risks.

Fitch Ratings-New York/Austin-18 June 2024: Cyber risk looms large for the water and sewer utility sector as a whole, but may not be as consequential for our rated portfolio, which is composed mostly of larger, highly-rated utilities that are well positioned with robust financial profiles and experienced management to address the risks and regulatory requirements, says Fitch Ratings. The median rating for our rated portfolio is 'AA+', with about 89% of the portfolio on Stable Rating Outlook and around 7% on Positive.

Water and sewer utilities are vulnerable to cyber breaches given their use of a number of complex and diverse operating and technology systems that make it challenging to guard against attacks. This risk is particularly acute for small systems with thin margins and limited staff. To date, however, none of the water and sewer systems rated by Fitch have been subject to negative rating action as a result of a cyber breach.

Fitch's criteria consider event risks such as cyber-attacks as asymmetric additive risks, where the focus is on the robustness of governance systems and protocols to counteract or mitigate the threat, and the utility management's reaction if an attack occurs.

Fitch may take negative rating action if a utility's financial profile is deemed to be materially impaired in the aftermath of a breach. Expenses associated with a cyber breach, including remediation and enhanced security measures, along with increased cybersecurity insurance premiums, legal costs and staffing and regulatory compliance expenses, could add to a utility's operating costs, erode liquidity and decrease funds available for debt service. Unexpected borrowing to bolster cybersecurity infrastructure, including updating compromised hardware and software systems, may further weaken leverage metrics.

A cyberattack that affects a utility's ability to provide service and/or hinders customer billing could temporarily reduce revenue generation for the system. Depending on the extent of the disruption, Fitch's assessment of the utility's revenue defensibility could be lowered.

A cyber breach could compound expense pressures for water utilities already facing greater demands on their budgets from inflation, aging infrastructure and EPA mandates to replace lead service lines and remove/reduce per- and polyfluoroalkyl substances from drinking water. To address increased expenses, utilities often raise rates, which, if further increased to recover cyber costs, could erode rate affordability.

The level of cyber risk among water utilities varies significantly against a backdrop of little federal or state regulation relative to the public power sector. Water and wastewater utilities would be obligated to report cyber incidents and ransomware payments to the Cybersecurity and Infrastructure Security Agency according to proposed rules issued on April 4, 2024. Public comment for these rules ends on July 3. In addition, a bill introduced in the House in April would create a Water Risk and Resiliency Organization to develop and enforce cyber risk and resiliency

requirements for water treatment and wastewater systems.

The trend towards smart infrastructure and the Internet of Things means that more water utility components are connected to the internet. This connectivity increases efficiency but also expands the attack surface. The use of homogenous operational technology (OT) across processes/systems also increases risk. Once hackers can exploit vulnerabilities in a certain system, they can often apply those techniques to other systems with the same OT.