Bond Case Briefs

Municipal Finance Law Since 1971

Fitch: US Federal Cyber Plan Could Help Mitigate Water Utility Cyber Risk

Fitch Ratings-Austin/New York-10 February 2022: Recent steps taken by the US federal government to bolster cyber resiliency across the water sector are an important start in mitigating rising cyber risks for publicly-owned utility systems, Fitch Ratings says.

The White House and Environmental Protection Agency (EPA) announced on Jan. 27 a new "action plan" that aims to encourage water utilities to adopt technology that detects cyber threats to industrial control systems (ICS), such as supervisory control and data acquisition (SCADA) applications. ICS systems were not generally engineered with cyber resiliency in mind and remain vulnerable to cyber intrusions. The federal plan recognizes that the reliance of the water sector on ICS, and the susceptibility of these systems to infiltration, constitutes a national security concern.

The federal government will initially pilot the program with utilities serving the largest population centers. The program will help utilities in their efforts identify, report and address cyber vulnerabilities, with support from the EPA and the Cybersecurity and Infrastructure Security Agency (CISA). Although the federal plan is unfunded, collaboration with the EPA and CISA may keep cyber security costs lower for utilities than if they were responsible for implementing cyber protections on their own. Technology improvement costs ultimately will be borne by the utilities and recovered from ratepayers.

The public water sector has not historically benefitted from coordinated federal cyber defense strategy or support, with limited national mandatory standards to ensure progress on a nationwide basis. As a result, the levels of cyber resiliency and risk preparedness at the nation's roughly 50,000 public water and wastewater systems vary widely. Water sector associations, such as the American Water Works Association (AWWA) and the Water Risk & Resilience Organization (WRRO), provided valuable cyber security guidance to their members in recent years but the programs have only a limited effect without robust legislative support.

In contrast, the power sector has been the focus of federal support and regulation for grid security and cyber resiliency for over a decade. Federal requirements for power utility cyber resiliency are set by the North American Electric Reliability Council (NERC) as part of their critical infrastructure protection (CIP) standards. The NERC-CIP standards have long been an effective bulwark of cyber resiliency for critical infrastructure and resulted in robust planning, regular federal investment and lower risk for the power sector.

Cyber risk can be an important consideration in our assessment of municipal utility systems' credit quality. Cyberattacks that halt service, delay revenue generation, require ransomware payments, or necessitate unexpected capital costs could negatively affect utility financial performance and result in widespread public and private sector shutdowns. Critical utilities are tempting targets for cybercrime, where successful breaches can be high impact, disruptive and lucrative.

Fitch considers whether utilities maintain cyber security policies and conduct training; budget for

necessary cyber security investment; maintain adequate insurance against cyberattack; and have protocols for addressing cyber incidents. The inability to adequately protect infrastructure from an attack is considered in our public utility criteria as part of our assessment of the quality of management and governance, which is an asymmetric risk where weaker characteristics may constrain a rating.

The federal effort to bolster water utility cyber resiliency is timely, as the US Department of Homeland Security (DHS) warned in a Jan. 23 memorandum that operators of public infrastructure could be increasingly targeted as a result of geopolitical tensions. Similar warnings were issued by the US Federal Bureau of Investigation and CISA in the past several weeks as global conflicts intensified.