Warner Requests Answers Following Concerning Cyber Breach on Florida Water Plant

warner.senate.gov/public/index.cfm/2021/2/warner-requests-answers-following-concerning-cyber-breach-on-florida-water-plant

WASHINGTON – U.S. Sen. Mark R. Warner, Chairman of the Senate Select Committee on Intelligence, today requested information from the Federal Bureau of Investigation (FBI) and the Environmental Protection Agency (EPA) following a cyber incident in which hackers remotely breached a Florida water treatment plant and sought to dramatically alter water chemical levels in a move that could have poisoned thousands of residents.

"The security and integrity of our critical infrastructure is of utmost importance. The Cybersecurity & Infrastructure Security Agency (CISA) states that 80% of the United States receives potable water from approximately 153,000 public drinking water systems, and any type of attack, including a cyber attack, could result in 'illnesses or casualties and/or a denial of service that would also impact public health and economic vitality,'" **wrote Sen. Warner in a letter to the Assistant Director of the FBI and the Acting Assistant Administrator at the EPA.** "This incident has implications beyond the 15,000-person town of Oldsmar. While the Oldsmar water treatment facility incident was detected with sufficient time to mitigate serious risks to the citizens of Oldsmar, and appears to have been identified as the result of a diligent employee monitoring this facility's operations, future compromises of this nature may not be detected in time."

He continued, "The Federal Government must ensure we are taking all precautions to keep drinking water safe for Americans. Designated as one of the 16 infrastructure sectors critical to national security under the Presidential Policy Directive 21 (PPD-21), we must protect water facilities from cyber and other compromises."

On February 5, a water treatment facility in Oldsmar, Florida was accessed remotely by hackers, who increased sodium hydroxide levels from 100 parts per million to 11,100 parts per million, a dangerous amount that could have sickened town residents, had the attack gone unnoticed by a plant employee.

In his letter, Sen. Warner requested a progress update on the FBI's investigation into this incident. He also asked for an EPA review into whether the Oldsmar water treatment facility was compliant with the most recent Water and Wastewater Sector-Specific Plan, and whether that plan needs to be updated to confront similar risks. Additionally, Sen. Warner inquired about any plans to share timely threat information related to this incident with water and wastewater facilities, and other critical infrastructure providers.

Sen. Warner, a former technology executive, is the co-founder and co-chair of the bipartisan Senate Cybersecurity Caucus. Throughout the COVID-19 crisis, he has fought for increased cybersecurity measures commensurate with Americans' increased reliance on remote work. Among other measures, Sen. Warner has advocated for increased funding to modernize federal information technology, urged internet networking device vendors to ensure the security of their products, and pressed cybersecurity officials to bolster defenses against cybersecurity attacks.

A copy of the letter can be found here and below.

Dear Mr. Gorham and Ms. Fox,

I am writing to request information about reports of a serious security compromise of a water treatment plant in Oldsmar, Florida on February 5, 2021. The security and integrity of our critical infrastructure is of utmost importance. The Cybersecurity & Infrastructure Security Agency (CISA) states that 80% of the United States receives potable water from approximately 153,000 public drinking water systems, and any type of attack, including a cyber attack, could result in "illnesses or casualties and/or a denial of service that would also impact public health and economic vitality."[i] Additionally, other critical infrastructure sectors such as healthcare, emergency services, energy, food and agriculture, and transportation systems depend on the cyber resilience of water facilities.[ii]

According to information released by the Pinellas County Sheriff's Office, the Oldsmar water treatment facility was accessed remotely by an unauthorized entity, who increased the amount of sodium hydroxide in the potable water supply to a dangerous level.[iii] Given the consequences of a successful compromise of this kind, and the broader security weaknesses this unsuccessful attempt may illustrate within critical infrastructure sectors

reliant on similar industrial control systems, I would request first, to be informed of the progress of the FBI's investigation of the incident; second, a review by the Environmental Protection Agency into whether the Oldsmar water treatment facility was compliant with the most recent Water and Wastewater Sector-Specific Plan, and whether that plan, most recently updated in 2015, needs to be updated to confront similar risks; and third, to confirm the Federal Government is sharing timely threat information related to this incident with water and wastewater facilities, and other critical infrastructure providers across the United States.

This incident has implications beyond the 15,000-person town of Oldsmar. While the Oldsmar water treatment facility incident was detected with sufficient time to mitigate serious risks to the citizens of Oldsmar, and appears to have been identified as the result of a diligent employee monitoring this facility's operations, future compromises of this nature may not be detected in time. The Federal Government must ensure we are taking all precautions to keep drinking water safe for Americans. Designated as one of the 16 infrastructure sectors critical to national security under the Presidential Policy Directive 21 (PPD-21), we must protect water facilities from cyber and other compromises.

Please coordinate with my office to provide updates on the investigation of the incident, as well as efforts underway to avoid future compromises on water facilities in the United States.

###