SolarWinds Cybersecurity Exploit: What Water Providers Need to Know and Do

12.17.2020 | By Willis Hon, Hon. Chris Carney

In light of the major cybersecurity breach of the SolarWinds Orion software by malicious actors, the Water Information Sharing and Analysis Center (WaterISAC) recently issued a series of advisories providing guidance for water providers across the country on how to respond and react to this unprecedented cyberattack.

As highlighted in the WaterISAC advisory issued on December 16, 2020, the Environmental Protection Agency has recommended that all water and wastewater utilities review the Cybersecurity and Infrastructure Security Agency's (CISA's) Emergency Directive 21-01 for mitigation procedures. While Emergency Directive 21-01 is specifically directed at federal agencies, it provides helpful steps that water providers can take to mitigate the potential impacts of this widespread attack that has impacted major international institutions.

The latest information about the SolarWinds cybersecurity exploit can be found on the website about this incident maintained by SolarWinds. It was first reported to the National Security Agency by cybersecurity firm FireEye, who has published a detailed blog post on this incident and shared a GitHub page with recommended detection countermeasures.

The incoming Biden Administration, echoing testimony this week on Capitol Hill from the former head of the Department of Homeland Security's CISA, stated that cybersecurity must be a top priority for the incoming Administration and Congress because America is vulnerable. We will continue to track and provide updates on this topic.