LELWD Publicizes Case Study on Foreign Hackers Targeting U.S. Utilities

LITTLETON, MA (March 14, 2025) – The Littleton Electric Light and Water Departments has participated in a case study with its cybersecurity provider that details the immediate steps taken to protect its computer networks after a 2023 intrusion by foreign hackers. There was no serious threat to public safety or customer data, and LELWD hopes publicizing the problem and solution helps utilities of all sizes act on the threats posed by foreign adversaries.

Here are key points to consider:

- No customer-sensitive data was compromised.

- In November 2023, the FBI alerted the LELWD that a Chinese cyberespionage group, Volt Typhoon, had access to its system. At that time, investigators told the LELWD that about 200 New England organizations were similarly affected.

- The LELWD took immediate action and cooperated with the U.S. Cybersecurity and Infrastructure Security Agency (CISA) to install sensors to monitor the activity of the hackers. While in the system, it appeared the hackers accessed a file server that stores public records.

- By December 2023, the federal government and the hackers were off the system. Last August, CISA returned to the LELWD to perform a two-week penetration test that showed the cybersecurity defenses working properly.

- The LELWD is a distribution company, and its systems do not have access to or control of the larger, critical electrical grid infrastructure. It appears the LELWD was targeted simply because its system used a firewall with a known security flaw. The then-managed service provider had not updated the firmware and as a result, was terminated.

- The LELWD was already bolstering its cybersecurity to better monitor operational technology (OT) assets, security information technology and OT network traffic, and monitor communications between OT devices and systems. OT systems are used to control and manage physical equipment and processes.

- The LELWD now contracts with managed served provider EvoLab Technology Solutions and uses a system monitoring platform from Dragos, Inc., a provider of OT cybersecurity technology for industrial and critical infrastructure. In addition, the LELWD's network architecture was changed to render unusable any system information potentially obtained by the hackers.

"We were able to quickly isolate the threat in late 2023 before anything happened, and we accelerated our ongoing work to strengthen our cybersecurity. We worked with the U.S. Department of Homeland Security's CISA, the FBI, the American Public Power Association, and our cybersecurity partners, EvoLab and Dragos, to protect our systems. We can now publicize this threat and solution to educate other small utilities. You would never think that you'd be targeted, but there is a real threat from foreign adversaries," said Nick Lawler, General Manager of the LELWD.

The cybersecurity improvements were led by David Ketchen, Assistant General Manager, whose efforts were recognized by the state's Executive Office of Technology Services & Security. Ketchen received the Cybersecurity & Risk Management award at the Massachusetts Excellence in Technology Awards in September 2024.

The LELWD was supported by the American Public Power Association, a national organization representing municipal electric utilities nationwide. Though its cybersecurity programs, the APPA has awarded more than $14 million to 32 utilities, funding 78 cybersecurity projects.

"The response to the LELWD breach was swift, according to Dragos. Investigators identified the attacker's movements, including server message block traversal and remote desktop protocol lateral movement," reported Infosecurity Magazine. "The compromised organization was able to contain the threat and reconfigure its network to prevent further exploitation. No customer-sensitive data was reportedly compromised."

###