FLOWPOINT®

OFFICIAL CLIENT COMMUNICATION

CLIENT ADVISORY NOTICE

July 8, 2026

SUBJECT: Important - U.S. Department of Homeland Security Cybersecurity Guidance for Industrial Control Systems

Dear [Customer Name],

You are being provided with this information as regards the recently issued U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) guidance (CISA on June 16, 2026 republished the Rockwell Automation Security Advisory SD1776 as ICSA-26-167-04 regarding Industrial Control Systems (ICS), specifically Rockwell Automation CompactLogix controllers that communicate using the Ethernet/IP protocol). The advisory states that these devices should not be directly exposed to the public internet without implementing appropriate network security measures to reduce cybersecurity risks.

At Flowpoint Systems, cybersecurity has always been a critical component of our system design. Our software requires secure communications with your station to provide monitoring, data collection, alarm notification, and remote support. While this requires a known network address, to help you ensure that your system remains in compliance with current cybersecurity leading practices, we are providing information in this document to help you ensure continued protection of the reliability, availability, and security of your water treatment system.

Questions or configuration review

If you have any questions regarding this information or would like to discuss your system's cybersecurity configuration further, please contact us.

Sincerely,

Gerry Assinger
Flowpoint Environmental Systems
1-877-655-5585 ext. 2
support@flowpointsystems.com

SECURE COMMUNICATIONS

Leading Practices

Flowpoint Systems is committed to protecting your water treatment system by following current industry cybersecurity leading practices. The communication options available depend on whether your system uses Client/Server Software or Flowpoint Cloud Software.

Client/Server Software

Client/Server software requires the client application to initiate communications with the station. Because the station must be accessible to software, we recommend one of the following communication methods, listed in order of preference.

1 Local Network Connection (Preferred)

When the station is connected to your organization's Local Area Network (LAN), the client software communicates over your private network. If remote access is required, it should be accomplished through your organization's existing VPN.

Benefits

- No direct internet exposure
- Uses your organization's existing security infrastructure
- Highest level of security

2 IP Whitelisting

If the station communicates over a cellular or Internet connection, the router can be configured to allow communications only from approved public IP addresses. Only authorized IP addresses - such as your office network and Flowpoint Support (when authorized) - are permitted to connect. All other connection attempts are ignored.

Benefits

- Simple to implement
- In most cases, no additional hardware is required
- Significantly reduces unauthorized access attempts
- Ideal when public IP addresses remain static

Client/Server Software - Continued

3 WireGuard VPN (Recommended)

WireGuard is a modern VPN protocol that provides secure, encrypted communications with minimal configuration and excellent performance.

Benefits

- End-to-end encrypted communications
- Minimal network exposure
- High performance and reliability
- Easier to configure and maintain than many traditional VPN solutions
- Recommended by Flowpoint for new Client/Server installations

4 Traditional VPN

A Virtual Private Network (VPN) creates a secure, encrypted tunnel between your office and the station.

Benefits

- Encrypted communications
- No direct access from the public internet
- Strong authentication
- Recommended for organizations with existing VPN infrastructure

FLOWPOINT CLOUD SOFTWARE

Flowpoint Cloud Software

Flowpoint Cloud software requires the application to initiate secure communications with the station. Because the station must be accessible to software, we recommend one of the following communication methods (listed in order of preference).

1 IP Whitelisting

Where supported by the router, configure a whitelist of trusted IP addresses to further restrict management access.

Benefits

- Limits access to authorized devices only
- In most cases, no additional hardware is required
- Reduces internet exposure
- Adds an additional layer of protection

2 WireGuard VPN (Recommended)

WireGuard provides a secure, encrypted connection for remote maintenance or administrative access without exposing the station directly to the public internet.

Benefits

- Secure encrypted remote access
- No publicly accessible controller ports
- Fast, lightweight, and highly secure
- Recommended for secure remote support

Our Commitment

Aligned with current CISA guidance

The recommendations align with CISA's guidance, which includes removing operational technology devices from direct internet exposure, implementing network segmentation, using secure remote access methods such as VPNs, restricting access to trusted sources, and following current cybersecurity leading practices. If your station is already configured using one of these communication methods, you are following current industry recommended practices for securing remote access. If you are unsure how your station is configured, or if you would like us to review your installation and recommend improvements, we would be pleased to assist.

DISTRIBUTION NOTICE

Distribution Notice

Recipient use only

This Client Advisory Notice is intended solely for the recipient(s). If you are not the intended recipient, please notify Flowpoint Environmental Systems immediately.

Flowpoint Environmental Systems
#467, 191 University Blvd | Denver, CO 80206-4613
877-655-5585 | support@flowpointsystems.com