

OPERATOR'S RAPID RESPONSE CHECKLIST

This guide is based on **CISA** and **EPA** advisories regarding active threats to U.S. water systems (e.g., Unitronics PLC exploitation).

1 THE "SEE IT" (Digital & Physical Indicators)

Category	Red Flag Indicator
HMI / Screen	Screen flickering, mouse moving on its own, or a political/ransom message appearing on the display.
PLC / Controller	The Unitronics or Pro-Face PLC screen shows a message like "You have been hacked" or "Down with Israel/USA."
Equipment	Pumps, valves, or chemical feeders turning on/off without a command or at unusual times.
Data/Sensors	Tank levels show "Normal" on the HMI, but physical inspection shows an overflow or a dangerously low level.
Network	Unexpected "remote access" sessions active on the workstation or slowed system performance.

2 THE "DO IT" (Immediate Mitigation Steps)

If you suspect a cyber-physical compromise, follow these steps in order:

- 1. GO TO MANUAL:** Immediately switch treatment and distribution to **manual override**. Do not rely on the HMI or PLC data until the system is cleared.
- 2. ISOLATE THE NETWORK:** Physically disconnect the affected HMI or PLC from the internet (unplug the Ethernet cable). **Do not** power down the device yet, as forensic evidence in the RAM may be lost.
- 3. ACTIVATE YOUR IRP:** If your organization has an Incident Response Plan (IRP), activate it immediately. Follow established notification, escalation, documentation, and containment procedures.
- 4. VERIFY WATER QUALITY:** Manually test chlorine residuals, pH, and turbidity. Ensure the "spoofed" digital data hasn't masked a chemical imbalance.
- 5. CHANGE PASSWORDS:** If you can still access the system, immediately change all **factory-default passwords** (e.g., 1111 or password) to unique, complex strings.

3 THE "REPORT IT" (Required Notifications)

- Local/State:** Contact the **New Hampshire State Police Cyber Crimes Unit** and the **NH Department of Environmental Services (NHDES)**.
- Federal:** Report the incident to the CISA Reporting Portal or call **(888) 282-0870**.
- Technical Support:** Request assistance from the **NH Municipal Cyber Defense Program** for a Continuity of Operations (COOP) Workshop to prevent a recurrence.

PRO-TIP: THE "GOLDEN IMAGE"

Coordinate with your SCADA Integrator and/or your Managed Service Provider to ensure you have a **physical or offline backup** of your PLC ladder logic and HMI configurations. If an attacker wipes your controller, "The Cloud" might be compromised too—keep a **USB drive in a locked safe** with your current verified configurations.