RAILROAD COMMISSION OF TEXAS

NOTICE TO ALL RRC REGULATED OPERATORS

Increased Possibility of Cyber Attacks

The Environmental Protection Agency (EPA) and the Cybersecurity and Infrastructure Security Agency (CISA) issued new advisories this week warning of an increased possibility of cyber attacks. These attacks are targeting internet-facing operational technology (OT) devices, including programmable logic controllers (PLCs) across US critical infrastructure potentially causing operational disruption and financial loss.

Some organizations in critical infrastructure sectors have already experienced disruptions caused by malicious interactions with the project files and the manipulation of data displayed on human machine interface (HMI) and supervisory control and data acquisition (SCADA) displays.

Recommended Actions from CISA
Operators should take the following steps to strengthen cyber resilience:

- Remove PLCs from direct internet exposure via secure gateway and firewall.
- Query available logs for the provided IOCs in the corresponding time frames.
- Check available logs for suspicious traffic on the ports associated with OT devices, including 44818, 2222, 102, and 502, especially traffic originating from overseas hosting providers.
- For Rockwell Automation devices
    - Place the physical mode switch on the controller into run position.
    - Contact the authoring agencies and Rockwell Automation for guidance if you believe your organization was targeted.

Additional Resources:

- EPA advisory: https://www.epa.gov/newsreleases/epa-fbi-cisa-nsa-issue-joint-cybersecurity-advisory-water-system-regarding-iranian.
- CISA advisory: https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-097a?utm_source=IranPLC202604&utm_medium=GovDelivery.

The RRC maintains a 24-hour, toll-free emergency line, 844-773-0305, to report emergencies, including leaks or spills and damage to gas pipelines.

Please Forward to the Appropriate Section of Your Company

Austin, Texas **April 2026**