LEGAL UPDATES

PUBLISHED: JULY 2, 2025

FBI Notes Increase in Cyber Activity Targeting Operational Technology

Service

Data Privacy & Cybersecurity

Industry

Manufacturing

Professional

ERIK DULLEA
DENVER:
303.749.7270
ERIK.DULLEA@
HUSCHBLACKWELL.COM

On June 30, 2025, the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), the National Security Agency (NSA), and the Department of Defense Cyber Crime Center (DC3) published a fact sheet, titled "Iranian Cyber Actors May Target Vulnerable US Networks and Entities of Interest," describing threats to U.S. critical infrastructure from Iranian cyber actors.

Using past as prologue, the fact sheet recaps the targeting in 2023 of program logic controllers and other operational technologies (OT) in the water and wastewater, energy, food and beverage manufacturing, healthcare, and public health sectors during the height of Israel-Hamas conflict by Iranian affiliates and proxies. The fact sheet is the latest communication from federal agencies urging the owners and operators of OT—particularly those in critical infrastructure sectors—to review, test, and improve their cybersecurity protocols.

In another recent example, the Environmental Protection Agency (EPA), Department of Energy (DOE), CISA, and FBI posted a fact sheet in May 2025, titled "Primary Mitigations to Reduce Cyber Threats to Operational Technology," summarizing cybersecurity best practices for enterprises that own or operate OT.

The May and June fact sheets offer similar recommendations to mitigate the risks to critical infrastructure and include:

Removing OT connections from the public internet;

Replacing manufacturers' default passwords on OT devices; and

Restricting and securing remote access to OT networks.

These mitigation efforts are vital because cyber incidents continue to grow in frequency with a corresponding increase in the costs of remediation and insurance premiums. Mitigation is crucial to managing the financial risks from cybercrime. However, for OT owners and operators, cyber risks are complex and can lead to various third-party liabilities and challenges beyond any single enterprise.

What this means to you

Owners and operators of internet-facing operational technology should take heed of the agencies' warnings and bolster both their mitigation efforts and their incident reporting protocols.

Contact us

If you have questions regarding the fact sheets, or how other cybersecurity developments could impact your business, contact Erik Dullea or your Husch Blackwell attorney.