BusinesSafe is designed to aid businesses in protecting the safety and well-being of Florida's residents and visitors from threats. BusinesSafe provides private sector partners with open source information, analysis and resources to help protect their businesses and communities.

Florida Fusion Center 22-020 **February 2022, Issue #71**

BusinesSafe Sector Highlight: Chemical Sector

The Chemical Sector manufactures, stores, uses, and transports chemicals to other critical infrastructure sectors across the United States. The Chemical Sector has interdependencies with other sectors including transportation, energy, water and wastewater, communication, and information technology. The federal government works closely with sector stakeholders to secure the Chemical Sector from harm.

Criminal Activity

Criminal actors may target the Chemical Sector to obtain proprietary information, steal hazardous chemicals for nefarious purposes, or attempt to disrupt operations with the intent to harm or for financial gain.

1. **Insider threat -** Employees in the Chemical Sector may have direct access to proprietary or other sensitive information. Some insiders may intentionally use their access to illegally obtain this information for financial gain. Insiders with access to this information may also become targets for criminal actors using them to obtain intellectual property for financial gain or a competitive edge, which can cause long term harm. This can include criminal actors sending phishing emails containing malicious links, which employees may click on giving the criminal actor unintentional access to company information systems.
   Ph.D. Chemist Convicted of Conspiracy to Steal Trade Secrets, Economic Espionage, Theft of Trade Secrets and Wire Fraud
   Four Chinese Nationals Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property

2. **Cyberattacks -** Chemical facilities rely on information network systems for facility operations, and can be targeted by cyberattacks carried out by criminal actors or nation-state actors. Both criminal actors and nation-state actors may carry out attacks for financial gain, access to proprietary information, or disruption of operations. Criminal actors may use password guessing, distributed denial of service attack, phishing emails, or other types of cyberattacks which can disrupt operations or give the criminal actors access to company information systems. The Chemical Sector works closely with industry and federal partners to ensure cybersecurity and mitigation against these types of attacks.
   Siegfried, Brenntag, and Symrise hit by cyberattacks
   Major U.S. Chemical Firms Hit by Cyberattack

Florida Fusion Center
(800) 342-0820
FLBusinesSafe@FDLE.state.fl.us

Author: FL8642, Approval: FL8600, HSEC:1, 2, 8 FSIN:1.1, 1.1.2, 1.1.4, 1.2.1, 1.10,2.6.1, 2.7.2 FFC: 1.1, 1.2, 1.3, 1.4, 1.7, 1.14, 2, 4.3, 6.9, 7.4

Other Threats or Hazards

1. **Natural or manmade hazards -** While chemical facilities are built to mitigate against the threats posed by natural hazards, unexpected incidents can result in operation disruptions. The chemicals produced or stored within these facilities can pose a threat to the public and environment if a natural or manmade hazard were to result in a chemical release, operation disruption, or fire. These disruptions can also reduce the facilities' ability to produce and distribute chemicals to other dependent sectors. Still, the Chemical Sector continues to increase mitigation and security techniques to ensure ongoing resilience against natural and manmade hazards.
   North Carolina fertilizer plant fire causes fear of explosion, area evacuated
   Oil, Chemical Plants Released Tons of Pollutants While Shutting Down for Hurricane Laura

2. **Bomb-making materials acquisition -** Terrorist or criminal actors may use the chemicals sold at retail stores or chemical distributors to produce improvised incendiary or explosive devices with the intent to harm others. Businesses are encouraged to have processes and procedures in place to identify and report suspicious activity regarding hazardous chemicals to the public to help prevent attacks.
   State of Bombing Prevention: Partnerships Are Key to Mitigate IED Threat
   Police, FBI raid Storrs man's home, find bomb-making materials, guns

Resources

- The Cybersecurity and Infrastructure Security Agency (CISA) offers extensive information for the Chemical Sector including safety and security resources for small to midsize facilities, training, and industry partnerships. CISA also offers resources for businesses on bomb prevention measures through their bomb-making materials awareness program.

- **"If You See Something, Say Something®"** – Report suspicious activity to your local law enforcement agency, on the FDLE website using Florida's See Something, Say Something Tool Kit, via the Florida See Say app, or by calling 855-FLA-Safe. In an emergency, call 911. FDLE also offers potential indicators of suspicious activities related to businesses selling chemical products and other possible threats to the Chemical Sector.

Florida Fusion Center
(800) 342-0820
FLBusinesSafe@FDLE.state.fl.us
Author: FL8642, Approval: FL8600, HSEC:1, 2, 8 FSIN:1.1, 1.1.2, 1.1.4, 1.2.1, 1.10,2.6.1, 2.7.2 FFC: 1.1, 1.2, 1.3, 1.4, 1.7, 1.14, 2, 4.3, 6.9, 7.4