

BUSINESSSAFE

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

Florida Fusion Center 20-221

November 2020, Issue #37

BusinessSafe Highlight: Defense Industrial Base

Criminal Activity

The Defense Industrial Base is the system that supports the research, development, design, construction, distribution, and maintenance of weapons systems and defense components for the U.S. military. Most defense industrial base facilities are owned and operated by a variety of domestic and foreign private entities with a small percentage owned by the Department of Defense. Criminal cyber actors and foreign adversaries may attempt to target the defense industrial base sector for financial gain or to advance a state's specific goals.

1. **Cyberattacks** – Cyber criminals continue to launch cyberattacks targeting the defense industrial base sector in order to gain access to sensitive information and technologies. Foreign adversaries may have a strategic interest in this sector due to the technology and defense information that may be housed on defense networks. Cyber criminals continue to use phishing and ransomware attacks against the defense industrial base sector to gain sensitive network credentials and for financial gain.

[Cyber Criminals Don't 'Brake' for Pandemics
2019 Cybersecurity Report](#)

Other Challenges

The Defense Industrial Base Sector may also face challenges due to its complex structure and sensitive functions which may impact the sector's physical and information security.

1. **Supply Chain Challenges** – The defense industrial base's supply chain is comprised of a variety of foreign and domestic suppliers who provide raw materials, equipment, and finished products to the sector. A number of challenges including fraudulent products, network vulnerabilities, and unauthorized extraction of sensitive data may have an impact on the integrity of products and services provided by these suppliers to the defense industry.

[DOD Takes Steps to Safeguard Supply Chain](#)



Florida Fusion Center
(800) 342-0820

FLBusinessSafe@FDLE.state.fl.us

Author: FL8507, Approval: FL8600, HSEC-1, FSIN-1

Resources

The Defense Security Service's Center for Development of Security Excellence provides guidance on supply chain risk management.

[Deliver Uncompromised: Supply Chain Risk Management](#) (PDF)

The Department of Defense's DOD-Defense Industrial Base Collaborative Information Sharing Environment serves to receive all cyber incident reporting affecting DOD contractor unclassified networks.

[DOD-Defense Industrial Base Collaborative Information Sharing Environment](#)

To sign up to receive [BusinessSafe](#) directly to your email, visit our [website](#).



Florida Fusion Center
(800) 342-0820

FLBusinessSafe@FDLE.state.fl.us

Author: FL8507, Approval: FL8600, HSEC-1, FSIN-1