

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 21-137

November 2021, Issue #64

BusinessSafe Infrastructure Security Month

November is Infrastructure Security Month, the goal of which is to educate the public and infrastructure owners and operators about the role of critical infrastructure and the importance of strengthening its security and resilience. The Cybersecurity and Infrastructure Security Agency (CISA) has designated this year's theme as "Build It In" as a reminder that security and resilience should be considered from the infrastructure's design concept through to its daily operations. CISA offers more information on its Infrastructure Security Month on their [website](#).

Threats

Critical infrastructure faces many different threats, and operators implement a multitude of security and mitigation measures to ensure continued security and resilience against these threats. The article touches on just a few of the most common types of threats these sectors face but is not all-encompassing.

1. **Cyber** – Cyber attacks have become a prominent threat to critical infrastructure, and may include ransomware, phishing, spear phishing, exploitation of remote desktop protocol weaknesses, and other types of attacks. These attacks have the potential to disrupt operations or harm others. Critical infrastructure operators and owners use multiple mitigation techniques and tools to protect themselves from these types of attacks.

[One password allowed hackers to disrupt Colonial Pipeline](#)
[Boston Children's Hospital DDoS Attacker Convicted](#)

2. **Targeted Attacks** – Bad actors may use physical attacks, including the use of improvised explosive devices (IEDs), arson, vehicle ramming and other attack methods, to harm infrastructure sector assets, facilities, or employees. These types of attacks can cause prolonged service outages, disrupt business operations harm employees, and impacts to one sector can interrupt or harm other sector operations.

[5G coronavirus conspiracy theory leads to 77 mobile towers burned in UK](#)
[FBI Investigating Possible Attack On Natural Gas Line In Aspen](#)



Florida Fusion Center
 (800) 342-0820

FLBusinessSafe@FDLE.state.fl.us

Author: FL8642, Approval: FL8600, HSEC: 1, 2, 8, FSIN: 1.1, 1.2.1, 1.10, 1.14, 2.6.1, 2.14, FFC: 1, 2, 6, 7.1, 7.2, 7.4

- 3. Insider Threat** – Infrastructure sector operators’ employ many people across the United States. Those with access to and knowledge of sector specific operations and security, can pose a threat, whether intentionally or unintentionally, and cause harm or damage. Insider threats can range from impacting operations to unauthorized use of customer information or assets.

[Maryland Nuclear Engineer and Spouse Arrested on Espionage-Related Charges](#)
[Insider Threats: An Age-Old Problem](#)

- 4. Natural Disasters** – Natural disasters can range in type and some sectors may be more susceptible to natural disasters than others. Some sectors may experience operation or production disruptions while disruption of others can lead to physical harm to those in the surrounding area. Facility operators work to ensure their facilities are able to withstand and resume operation following natural disasters.

[Why a predictable cold snap crippled the Texas power grid](#)
[Hurricane Ida hit the oil industry hard as it headed to New Orleans](#)

Resources:

- CISA provides different ways for organizations and individuals to build in security and resilience as well as a [toolkit](#) with in-depth information and resources. A few other resources CISA offers include:
 - Information on the [National Critical Functions](#) of the government and private sector to protect the interconnected web of critical infrastructure dependencies and interdependencies against potential threats, including resources on risks and mitigation strategies.
 - [Critical infrastructure training](#) to help individuals and businesses better understand and implement critical infrastructure security and resilience activities.
 - Resources for organizations to help [secure public gathering](#) spaces and mitigate risks.
 - A guide on the [Infrastructure Resilience Planning Framework](#) to help organizations incorporate security and resilience into their facility and operations.
 - [Cybersecurity](#) best practices for infrastructure operators.

Each citizen has a part to play in ensuring that our critical infrastructure sectors are secure and resilient and continue to provide essential services. Find out more on www.BusinessSafe.org.



Florida Fusion Center
 (800) 342-0820

FLBusinessSafe@FDLE.state.fl.us

Author: FL8642, Approval: FL8600, HSEC: 1, 2, 8, FSIN: 1.1, 1.2.1, 1.10, 1.14, 2.6.1, 2.14, FFC: 1, 2, 6, 7.1, 7.2, 7.4