

## Committee on Criminal Justice

### **CS/CS/CS/HB 275 — Offenses Involving Critical Infrastructure**

by Judiciary Committee; Energy, Communications & Cybersecurity Subcommittee; Criminal Justice Subcommittee; and Rep. Canady and others (CS/CS/CS/SB 340 by Fiscal Policy Committee; Regulated Industries Committee; Criminal Justice Committee; and Senator Yarborough)

The bill creates s. 812.141, F.S., relating to offenses involving critical infrastructure. The bill creates new felony offenses and provides for civil remedies if a person is found to have improperly tampered with critical infrastructure.

The bill defines “critical infrastructure” to mean any linear asset or any specified entities for which the owner or operator thereof has employed measures designed to exclude unauthorized persons, including, but not limited to, fences, barriers, guard posts, or signs prohibiting trespass.

“Improperly tampers” means to cause, or attempt to cause, significant damage to, or a significant interruption or impairment of a function of, critical infrastructure without permission or authority to do so.

A person commits a second degree felony if he or she knowingly and intentionally improperly tampers with critical infrastructure which results in:

- Damage to such critical infrastructure that is \$200 or more; or
- The interruption or impairment of the function of such critical infrastructure which costs \$200 or more in labor and supplies to restore.

The bill provides that a person who is found in a civil action to have improperly tampered with critical infrastructure based on a conviction of the above described crime is liable to the owner or operator of the critical infrastructure.

A person commits a third degree felony crime of trespass if he or she, without being authorized, licensed, or invited, willfully enters upon or remains upon critical infrastructure as to which notice against entering or remaining in is given.

A person commits a third degree felony if he or she willfully, knowingly, and without authorization gains access to a computer, computer system, computer network, or electronic device owned, operated, or used by any critical infrastructure entity, while knowing that such access is unauthorized.

A person commits a second degree felony if he or she willfully, knowingly, and without authorization physically tampers with, inserts a computer contaminant into, or otherwise transmits commands or electronic communications to a computer, computer system, computer network, or electronic device that causes a disruption in any service delivered by any critical infrastructure.

If approved by the Governor, or allowed to become law without the Governor's signature, these provisions take effect July 1, 2024.

*Vote: Senate 39-0; House 110-5*