



26        2. Any of the following for which the owner or operator  
27 thereof has employed physical or digital measures designed to  
28 exclude unauthorized persons, including, but not limited to,  
29 fences, barriers, guard posts, identity and access management,  
30 firewalls, virtual private networks, encryption, multifactor  
31 authentication, passwords, or other cybersecurity systems and  
32 controls:

33        a. An electric power generation, transmission, or  
34 distribution facility, or a substation, a switching station, or  
35 an electrical control center.

36        b. A chemical or rubber manufacturing or storage facility.

37        c. A mining facility.

38        d. A natural gas or compressed gas compressor station,  
39 storage facility, or pipeline.

40        e. A gas processing plant, including a plant used in the  
41 processing, treatment, or fractionation of natural gas.

42        f. A liquid natural gas or propane gas terminal or storage  
43 facility with a capacity of 4,000 gallons or more.

44        g. Any portion of an aboveground oil or gas pipeline.

45        h. A wireless or wired communications network, including  
46 the tower, antennae, support structures, and all associated  
47 ground-based equipment, including equipment intended to provide  
48 communications to governmental entities, including, but not  
49 limited to, law enforcement agencies, fire emergency medical  
50 services, emergency management agencies, or any other

51 governmental entity.

52 i. A water intake structure, water treatment facility,  
53 wastewater treatment plant, pump station, or lift station.

54 j. A deepwater port, railroad switching yard, airport,  
55 trucking terminal, or other freight transportation facility.

56 k. A facility used for the operation, landing, takeoff, or  
57 surface maneuvering of vehicles, aircraft, or spacecraft.

58 l. A transmission facility used by a federally licensed  
59 radio or television station.

60 m. A military base or military facility conducting  
61 research and development of military weapons systems,  
62 subsystems, components, or parts.

63 n. A civilian defense industrial base conducting research  
64 and development of military weapons systems, subsystems,  
65 components, or parts.

66 o. Cyber or virtual assets, including electronic systems,  
67 networks, servers, data centers, devices, hardware, software, or  
68 data that are essential to the reliable operations, monitoring,  
69 and security of any critical infrastructure.

70 p. Dams and other water control structures.

71 (b) "Improperly tampers" means to knowingly and  
72 intentionally cause, or attempt to cause, a significant  
73 interruption or impairment of a function of critical  
74 infrastructure by:

75 1. Changing the physical location or physical or virtual

76 condition of the critical infrastructure, or any portion  
 77 thereof, without permission or authority to do so;

78 2. Otherwise moving, damaging, or destroying the critical  
 79 infrastructure or any portion thereof, without permission or  
 80 authority to do so; or

81 3. Accessing without authorization, introducing malware,  
 82 or taking any other action that compromises the integrity or  
 83 availability of the critical infrastructure's digital systems.

84 (c) "Linear asset" means any electric distribution or  
 85 transmission asset, gas distribution or transmission pipeline,  
 86 communication wirelines, or railway, and any attachments  
 87 thereto.

88 (2) A person who improperly tampers with critical  
 89 infrastructure resulting in damage to critical infrastructure  
 90 that is \$200 or more or in the interruption or impairment of the  
 91 function of critical infrastructure which costs \$200 or more in  
 92 labor and supplies to restore, commits a felony of the second  
 93 degree, punishable as provided in s. 775.082, s. 775.083, or s.  
 94 775.084.

95 (3) A person who is found in a civil action to have  
 96 improperly tampered with critical infrastructure based on a  
 97 conviction for a violation of subsection (2) is liable to the  
 98 owner or operator of the critical infrastructure for damages in  
 99 an amount equal to three times the actual damage sustained by  
 100 the owner or operator due to any property damage, personal

101 injury, or wrongful death, caused by the act or an amount equal  
102 to three times any claim made against the owner or operator for  
103 any property damage, personal injury, or wrongful death caused  
104 by the malfunction of the critical infrastructure resulting from  
105 the act, whichever is greater.

106 (4) A person commits the offense of trespass on critical  
107 infrastructure, a felony of the third degree, punishable as  
108 provided in s. 775.082, s. 775.083, or s. 775.084, if he or she  
109 without being authorized, licensed, or invited, willfully enters  
110 upon or remains on physical critical infrastructure as to which  
111 notice against entering or remaining in is given, either by  
112 actual communication to the offender or by posting, fencing, or  
113 cultivation as described in s. 810.011.

114 (5)(a) A person who willfully, knowingly, and without  
115 authorization gains access to a computer, a computer system, a  
116 computer network, or an electronic device that is owned,  
117 operated, or used by any critical infrastructure entity while  
118 knowing that such access is unauthorized commits a felony of the  
119 third degree, punishable as provided in s. 775.082, s. 775.083,  
120 or s. 775.084.

121 (b) A person who willfully, knowingly, and without  
122 authorization physically tampers with, inserts a computer  
123 contaminant into, or otherwise transmits commands or electronic  
124 communications to, a computer, a computer system, a computer  
125 network, or an electronic device that causes a disruption in any

126 service delivered by any critical infrastructure commits a  
127 felony of the second degree, punishable as provided in s.  
128 775.082, s. 775.083, or s. 775.084.

129 (c) For purposes of this subsection, the terms "computer,"  
130 "computer system," "computer network," and "electronic device"  
131 have the same meanings as in s. 815.03.

132 Section 2. This act shall take effect July 1, 2024.