Florida Senate - 2006

By the Committee on Criminal Justice; and Senator Wise

591-1898-06

1	A bill to be entitled
2	An act relating to electronic monitoring;
3	amending s. 648.387, F.S.; authorizing bail
4	bond agents to be vendors of electronic
5	monitoring services; authorizing bail bond
6	agents to contract with third-party vendors to
7	provide electronic monitoring of pretrial
8	releasees in certain circumstances; authorizing
9	bail bond agents to register with a
10	governmental entity to provide electronic
11	monitoring services in certain circumstances;
12	authorizing such agents to collect a fee for
13	electronic monitoring services; providing that
14	failure to timely pay fees constitutes grounds
15	to remand; providing that such fees are exempt
16	from specified premium requirements; creating
17	s. 907.06, F.S.; providing for electronic
18	monitoring of certain persons on pretrial
19	release; requiring the monitored person to pay
20	fees; providing that provision of electronic
21	monitoring equipment and services is not an
22	undertaking to protect members of the public
23	from harm occasioned by a monitored person;
24	prohibiting a person being monitored from
25	tampering with monitoring equipment; creating
26	s. 907.07, F.S.; requiring the chief judge of
27	each circuit to maintain a list of licensed
28	bail bond agents who are eligible private
29	vendors for provision of electronic monitoring
30	services; requiring registration of such
31	vendors and certification of electronic

1

1	monitoring devices; providing grounds for
2	removal from the list; creating s. 907.08,
3	F.S.; providing standards for privately owned
4	electronic monitoring devices; creating s.
5	907.09, F.S.; providing criminal penalties for
6	tampering with electronic monitoring devices;
7	providing criminal penalties for cloning or
8	jamming the signal of an electronic monitoring
9	device; providing criminal penalties for the
10	alteration or destruction of data stored or
11	transmitted by an electronic monitoring device
12	with specified intent; creating ss. 944.161 and
13	985.4047, F.S.; providing for electronic
14	monitoring of inmates within correctional
15	facilities and juvenile offenders within
16	juvenile facilities, respectively; requiring
17	such monitoring of certain employees and
18	visitors to such facilities; providing system
19	requirements; prohibiting specified actions
20	relating to such monitoring systems and data
21	from such systems; providing penalties;
22	providing rulemaking authority; providing an
23	effective date.
24	
25	Be It Enacted by the Legislature of the State of Florida:
26	
27	Section 1. Section 648.387, Florida Statutes, is
28	amended to read:
29	648.387 Primary bail bond agents; duties <u>; electronic</u>
30	monitoring services by licensed bail bond agents
31	

1	(1) The owner or operator of a bail bond agency shall
2	designate a primary bail bond agent for each location, and
3	shall file with the department the name and license number of
4	the person and the address of the location on a form approved
5	by the department. The designation of the primary bail bond
б	agent may be changed if the department is notified
7	immediately. Failure to notify the department within 10
8	working days after such change is grounds for disciplinary
9	action pursuant to s. 648.45.
10	(2) The primary bail bond agent is responsible for the
11	overall operation and management of a bail bond agency
12	location, whose responsibilities may include, without
13	limitations, hiring and supervising of all individuals within
14	the location, whether they deal with the public in the
15	solicitation or negotiation of bail bond contracts or in the
16	collection or accounting of moneys. A person may be designated
17	as primary bail bond agent for only one location.
18	(3) The department may suspend or revoke the license
19	of the owner, operator, and primary bail bond agent if a bail
20	bond agency employs, contracts with, or uses the services of a
21	person who has had a license denied or whose license is
22	currently suspended or revoked. However, a person who has been
23	denied a license for failure to pass a required examination
24	may be employed to perform clerical or administrative
25	functions for which licensure is not required.
26	(4) An owner, operator, or primary agent may not
27	employ, contract with, or use the services of any person in a
28	bail bond agency who has been charged with, found guilty of,
29	or pled guilty or nolo contendere to a felony or a crime
30	punishable by imprisonment of 1 year or more under the law of
31	
	2

Florida Senate - 2006 591-1898-06

1 any jurisdiction, without regard to whether judgment was 2 entered or withheld by the court. (5) A bail bond agency location may not conduct surety 3 4 business unless a primary bail bond agent is designated at all times. The failure to designate a primary agent on a form 5 6 prescribed by the department, within 10 working days after an 7 agency's inception or a change of primary agent, is a 8 violation of this chapter, punishable as provided in s. 9 648.45. 10 (6)(a) A licensed bail bond agent who meets the requirements of s. 907.07 may be a vendor of electronic 11 monitoring services. A licensed bail bond agent may also 12 13 subcontract for such services with a third-party vendor of the bail bond agent's choice provided the licensed bail bond agent 14 can certify that the equipment and services rendered by such 15 third-party vendor on the bail bond agent's behalf meet the 16 17 requirements of s. 907.07 for monitoring of a defendant for 18 whom the bail bond agent has provided a criminal surety bail bond. A licensed bail bond agent who meets the requirements of 19 s. 907.07 may additionally register with a governmental entity 2.0 21 to provide electronic monitoring services when monitoring has 22 been ordered by a court. 23 (b) A licensed bail bond agent may charge a reasonable, nonrefundable fee for electronic monitoring 2.4 services from a person who is subject to electronic 25 monitoring. Failure to timely pay such fees constitutes 26 27 grounds for the agent to remand such person to the court or 2.8 sheriff. Fees charged by a bail bond agent associated with required electronic monitoring services are not considered 29 part of the bail bond premium and are exempt from the 30 provisions of s. 648.33. 31

4

1	(c) Records and receipts for electronic monitoring
2	provided by a licensed bail bond agent shall be kept separate
3	and apart from bail bond records.
4	Section 2. Section 907.06, Florida Statutes, is
5	created to read:
6	907.06 Electronic monitoring
7	(1) The court may order a defendant who has been
8	charged with a forcible felony, as defined in s. 776.08, or a
9	sex-related offense, or who has been charged with any crime
10	and who has been previously convicted of a forcible felony or
11	a sex-related offense, to be released from custody on a surety
12	bond subject to conditions that include, without limitation,
13	electronic monitoring, if electronic monitoring is available
14	in the jurisdiction. For purposes of this section, the term
15	"sex-related offense" includes any of the offenses contained
16	<u>in s. 943.0435(1)(a)1.</u>
17	(2) A defendant required to submit to electronic
18	monitoring shall pay a reasonable fee for equipment use and
19	monitoring as an additional condition of pretrial release. The
20	failure of the defendant to timely pay such fees constitutes a
21	violation of pretrial release and grounds for the defendant to
22	be remanded to the court or appropriate sheriff or law
23	enforcement agency.
24	(3) Electronic monitoring shall include the provision
25	of services to continuously receive and monitor the electronic
26	signals from the transmitter worn by the defendant so as to be
27	capable of identifying the defendant's geographic position at
28	any time to within 9 meters using Global Positioning Satellite
29	(GPS) technology, subject to the limitations related to the
30	technology and to circumstances of force majeure. Such
31	electronic monitoring services may be undertaken as a primary

1	responsibility by a governmental entity or by a licensed bail
2	bond agent who may provide both bail bond services and have
3	primary responsibility or oversight for electronic monitoring
4	services. A governmental entity or licensed bail bond agent
5	may subcontract to a third-party vendor for electronic
6	monitoring services, provided such third-party vendor complies
7	with all provisions of this subsection and s. 907.08 and
8	operates under the direction and control of the governmental
9	entity or licensed bail bond agent with primary responsibility
10	as the vendor for electronic monitoring. A governmental entity
11	that elects to subcontract for electronic monitoring services
12	shall be required to select such third-party vendor through a
13	competitive bidding process.
14	(4)(a) Any person who provides electronic monitoring
15	services shall report forthwith any known violation of the
16	defendant's pretrial release conditions to the appropriate
17	court, sheriff or law enforcement agency, state attorney, and
18	licensed bail bond agent, if any.
19	(b)1. Notwithstanding paragraph (a), the provision of
20	electronic monitoring services shall not be deemed to
21	constitute an undertaking to protect members of the public
22	from harm occasioned by a monitored person. The sole duty owed
23	by a person who provides electronic monitoring is to give a
24	law enforcement officer, upon request, an indication of the
25	physical location of the monitored person at any point in
26	time.
27	2. A person who provides electronic monitoring is not
28	responsible to other persons for equipment failure or for the
29	criminal acts of a monitored person. A provider of electronic
30	monitoring services cannot control the activities of a
31	monitored person. It is unreasonable for any member of the
	C

1	public to expect that a provider of electronic monitoring
2	services will provide protection against harm occasioned by a
3	monitored person.
4	(5) A defendant who has been released in accordance
5	with this section shall not alter, tamper with, damage, or
6	destroy any electronic monitoring equipment or data recorded
7	by such equipment. A defendant who is notified of a
8	malfunction in the equipment shall immediately cooperate with
9	the vendor in restoring the equipment to proper functioning. A
10	violation of this subsection constitutes a violation of
11	pretrial release and grounds for the defendant to be remanded
12	to the court or appropriate sheriff or law enforcement agency.
13	Section 3. Section 907.07, Florida Statutes, is
14	created to read:
15	907.07 Vendor requirements for provision of electronic
16	monitoring services; vendor registration and certification
17	process
18	(1) This section shall not apply to electronic
19	monitoring provided directly by the state, a county, or a
20	<u>sheriff.</u>
21	(2) The chief judge of each judicial circuit shall
22	maintain a list of all licensed bail bond agents who are
23	eligible vendors of electronic monitoring in the circuit. For
24	<u>a licensed bail bond agent to be an eligible vendor, a</u>
25	licensed bail bond agent must register in accordance with this
26	section as a vendor capable of providing electronic monitoring
27	services as a primary provider or through a subcontractor in
28	that judicial circuit. The chief judge shall place on such
29	list of eligible vendors any licensed bail bond agent in this
30	state who certifies in writing, as part of the vendor
31	registration, that all electronic monitoring equipment and

1 electronic monitoring services shall be operated and 2 maintained in compliance with this section, and who agrees as part of such certification to comply with the terms of this 3 4 section. 5 (3) Only a governmental entity, or a licensed bail 6 bond agent who is included on a list of eligible vendors under 7 subsection (2), shall be permitted to undertake primary 8 responsibility as a vendor of electronic monitoring services in a judicial circuit of this state. 9 10 (4) A licensed bail bond agent shall agree to abide by the following minimum terms as a condition of being included 11 12 on the list of eliqible vendors of electronic monitoring in a 13 given judicial circuit of this state: (a) The vendor shall register in writing the name of 14 the vendor, who must be a licensed bail bond agent in this 15 state; the name of an individual employed by the vendor who is 16 17 to serve as a contact person for the vendor; the address of 18 the vendor; and the telephone number of the contact person. 19 (b) The vendor must initially certify as part of the registration, and must certify in writing at least annually 20 21 thereafter on a date set by the chief judge, that all of the 2.2 electronic monitoring devices used by the vendor and any of 23 the vendor's subcontractors comply with the requirements for privately owned electronic monitoring devices in s. 907.08. 2.4 (5) A vendor shall promptly notify the chief judge of 25 any changes in the vendor's registration information that is 26 27 required under this section. 2.8 (6) Failure to comply with the registration or recertification requirements of this section shall be grounds 29 for removal from any chief judge's list of eligible vendors 30 for electronic monitoring. 31

8

1	(7) The chief judge, in his or her discretion, may
2	also remove any registered vendor from the list of eligible
3	vendors if the vendor:
4	(a) Fails to properly monitor any person that the
5	vendor was required to monitor; or
6	(b) Charges a defendant a clearly excessive fee for
7	use and monitoring of electronic monitoring equipment. Such
8	fees shall be considered clearly excessive if the fees charged
9	on a per diem basis are at least twice the average fee charged
10	by other vendors on the eligible vendor list who provide
11	comparable electronic monitoring equipment and services in
12	that judicial circuit.
13	Section 4. Section 907.08, Florida Statutes, is
14	created to read:
15	907.08 Standards for privately owned electronic
16	monitoring devicesA privately owned electronic monitoring
17	device provided by a vendor must, at a minimum, meet the
18	standards set forth in this section to be used for electronic
19	monitoring of a person under s. 907.06. A device must:
20	(1) Be a transmitter unit that meets certification
21	standards approved by the Federal Communications Commission.
22	(2) At the court's discretion, either:
23	(a) Emit signal content 24 hours per day that
24	identifies the specific device being worn by the defendant and
25	the defendant's physical location using Global Positioning
26	Satellite (GPS) technology accurate to within 9 meters; or
27	(b) Receive signal content 24 hours per day,
28	determining the defendant's physical location using Global
29	Positioning Satellite (GPS) technology accurate to within 9
30	meters, recording the defendant's physical locations
31	

1	throughout the day, and being capable of transmitting that
2	record of locations to the vendor at least daily.
3	(3) With respect to a unit affixed to a defendant,
4	possess an internal power source that provides a minimum of 1
5	year of normal operation without recharging or replacing the
6	power source. The device must emit signal content that
7	indicates its power status and provides the vendor with
8	notification of whether the power source needs to be recharged
9	or replaced.
10	(4) Possess and emit signal content that indicates
11	whether the transmitter has been subjected to tampering or
12	removal.
13	(5) Possess encrypted signal content or another
14	feature designed to discourage duplication.
15	(6) Be of a design that is shock resistant,
16	waterproof, and capable of reliable function under normal
17	atmospheric and environmental conditions.
18	(7) Be capable of wear and use in a manner that does
19	not pose a safety hazard or unduly restrict the activities of
20	the defendant.
21	(8) Be capable of being attached to the defendant in a
22	manner that readily reveals any efforts to tamper with or
23	remove the transmitter upon visual inspection.
24	(9) Use straps or other mechanisms for attaching the
25	transmitter to the defendant that are either capable of being
26	adjusted to fit a defendant of any size or that are made
27	<u>available in a variety of sizes.</u>
28	Section 5. Section 907.09, Florida Statutes, is
29	created to read:
30	907.09 Offenses related to electronic monitoring
31	devices
	1.0

1	(1) It is illegal for any person to intentionally
2	alter, tamper with, damage, or destroy any electronic
3	monitoring equipment used for monitoring the location of a
4	person pursuant to court order, unless such person is the
5	owner of the equipment or an agent of the owner performing
б	ordinary maintenance and repairs. A person who violates this
7	subsection commits a felony of the third degree, punishable as
8	provided in s. 775.082, s. 775.083, or s. 775.084.
9	(2) It is illegal for any person to develop, build,
10	create, possess, or use any device that is intended to mimic,
11	clone, interfere with, or jam the signal of an electronic
12	monitoring device used to monitor the location of a person
13	pursuant to court order. A person who violates this subsection
14	commits a felony of the third degree, punishable as provided
15	<u>in s. 775.082, s. 775.083, or s. 775.084.</u>
16	(3) A person may not intentionally alter, tamper with,
17	damage, or destroy any data stored or transmitted by any
18	electronic monitoring equipment used for monitoring the
19	location of a person pursuant to court order with the intent
20	to violate such court order or to conceal such a violation. A
21	person who violates this subsection commits a felony of the
22	third degree, punishable as provided in s. 775.082, s.
23	<u>775.083, or s. 775.084.</u>
24	Section 6. Section 944.161, Florida Statutes, is
25	created to read:
26	944.161 Electronic monitoring of inmates within
27	correctional facilities
28	(1) The department is authorized and encouraged to
29	employ electronic monitoring of inmates within its custody who
30	are incarcerated within state and private correctional
31	facilities.
	11

1	(a) Electronic monitoring services must have the
2	capability to continuously receive and monitor electronic
3	<u>signals from a transmitter worn by an inmate so as to</u>
4	continuously monitor the inmate in real time and identify the
5	inmate's specific geographic position within the facility at
б	any time. Such transmitters must update in at least 5-second
7	intervals and monitor the inmate's geographical location to
8	within at least a 10-foot radius of his or her actual location
9	or to within a radius that is equal to the width of a
10	facility's average size sleeping quarters, whichever is less,
11	subject to the limitations relating to the state of the art of
12	the technology used and to circumstances of force majeure.
13	(b) Any electronic monitoring system employed shall
14	also provide transmitters to be worn by department employees,
15	employees of private-sector companies contracted to operate
16	correctional facilities, and any visitors to correctional
17	facilities who are provided access to areas that are
18	designated for authorized personnel only. Such transmitters
19	shall include a panic safety button and must have the
20	capability to continuously receive and monitor electronic
21	<u>signals from a transmitter worn by an employee or visitor so</u>
22	as to continuously monitor employees and visitors in real time
23	and identify their specific geographic positions at any time.
24	Such transmitters must update in at least 5-second intervals
25	and monitor employees and visitors to within a 10-foot radius
26	of their actual location, subject to the limitations relating
27	to the state of the art of the technology used and to
28	circumstances of force majeure.
29	(c) Any electronic monitoring system employed shall
30	also have the following technological and functional
31	<u>capabilities:</u>

Florida Senate - 2006 591-1898-06

2wireless network access standard as designated by the3department and have sufficient bandwidth to support additional4wireless networking devices in order to increase the capacity5for usage of the system by the correctional facility.62. Be capable of issuing an alarm to an internal7correctional monitoring station within 3 seconds after8receiving a panic alert from an employee or visitor9transmitter or within 3 seconds after violation of the10established parameters for permissible movement of inmates,11sandowes, and visitors within the facility.123.a. Be capable of maintaining a historical storage13capacity sufficient to store up to 6 months of complete14inmate, employee, and visitor tracking for purposes of15follow-up investigations and vendor contract auditing. The18system must be capable of recording for such purposes the19selected individual, by specific position, not by area or10zone, Such historical information must also be capable of11being archived by means of electronic data transfer to a12permanent.13b. In addition, data collected from each facility each14shall be maintained in a secure storage location in a15permanent storage medium designated as acceptable by the16department as a supplemental backup in order to protect the17archived data from alteration and to prevent loss due to18individuals in a secure storage location in a<	1	1. Be compatible with a commercially recognized
 wireless networking devices in order to increase the capacity for usage of the system by the correctional facility. 2. Be capable of issuing an alarm to an internal correctional monitoring station within 3 seconds after receiving a panic alert from an employee or visitor transmitter or within 3 seconds after violation of the established parameters for permissible movement of inmates. employees, and visitors within the facility. 3.a. Be capable of maintaining a historical storage capacity sufficient to store up to 6 months of complete inmate, employee, and visitor tracking for purposes of follow-up investigations and vendor contract auditing. The system must be capable of recording for such purposes the continuous uninterrupted movement of all monitored individuals, including those in close proximity to any selected individual, by specific position, not by area or zone. Such historical information must also be capable of being archived by means of electronic data transfer to a permanent storage medium designated as acceptable by the department. b. In addition, data collected from each facility each day shall be electronically transmitted to an offsite central clearinghouse designated by the department where the data shall be maintained in a secure storage location in a permanent storage medium designated as acceptable by the department as a supplemental backup in order to protect the archived data from alteration and to prevent loss due to 	2	wireless network access standard as designated by the
5for usage of the system by the correctional facility.62. Be capable of issuing an alarm to an internal correctional monitoring station within 3 seconds after7receiving a panic alert from an employee or visitor9transmitter or within 3 seconds after violation of the established parameters for permissible movement of inmates, employees, and visitors within the facility.123.a. Be capable of maintaining a historical storage capacity sufficient to store up to 6 months of complete inmate, employee, and visitor tracking for purposes of follow-up investigations and vendor contract auditing. The system must be capable of recording for such purposes the continuous uninterrupted movement of all monitored individuals, including those in close proximity to any selected individual, by specific position, not by area or zone. Such historical information must also be capable of being archived by means of electronic data transfer to a permanent storage medium designated as acceptable by the day shall be electronically transmitted to an offsite central clearinghouse designated by the department where the data26gepartment.27b. In addition, as secure storage location in a permanent storage medium designated as acceptable by the28permanent storage medium designated as acceptable by the29gepartment as a supplemental backup in order to protect the archived data from alteration and to prevent loss due to	3	department and have sufficient bandwidth to support additional
 6 2. Be capable of issuing an alarm to an internal correctional monitoring station within 3 seconds after receiving a panic alert from an employee or visitor transmitter or within 3 seconds after violation of the established parameters for permissible movement of inmates, employees, and visitors within the facility. 3.a. Be capable of maintaining a historical storage capacity sufficient to store up to 6 months of complete inmate, employee, and visitor tracking for purposes of follow-up investigations and vendor contract auditing. The system must be capable of recording for such purposes the continuous uninterrupted movement of all monitored individuals, including those in close proximity to any selected individual, by specific position, not by area or zone. Such historical information must also be capable of being archived by means of electronic data transfer to a permanent storage medium designated as acceptable by the department. 4 b. In addition, data collected from each facility each day shall be electronically transmitted to an offsite central clearinghouse designated by the department where the data shall be maintained in a secure storage location in a permanent storage medium designated as acceptable by the department as a supplemental backup in order to protect the archived data from alteration and to prevent loss due to 	4	wireless networking devices in order to increase the capacity
7correctional monitoring station within 3 seconds after8receiving a panic alert from an employee or visitor9transmitter or within 3 seconds after violation of the10established parameters for permissible movement of inmates,11employees, and visitors within the facility.123.a. Be capable of maintaining a historical storage13capacity sufficient to store up to 6 months of complete14inmate, employee, and visitor tracking for purposes of15follow-up investigations and vendor contract auditing. The18system must be capable of recording for such purposes the17continuous uninterrupted movement of all monitored18individuals, including those in close proximity to any19selected individual, by specific position, not by area or20zone. Such historical information must also be capable of21being archived by means of electronic data transfer to a22permanent storage medium designated as acceptable by the23department.24b. In addition, data collected from each facility each25shall be electronically transmitted to an offsite central26clearinghouse designated by the department where the data27shall be maintained in a secure storage location in a28permanent storage medium designated as acceptable by the29department as a supplemental backup in order to protect the30archived data from alteration and to prevent loss due to	5	for usage of the system by the correctional facility.
8receiving a panic alert from an employee or visitor9transmitter or within 3 seconds after violation of the10established parameters for permissible movement of inmates.11employees, and visitors within the facility.123.a. Be capable of maintaining a historical storage13capacity sufficient to store up to 6 months of complete14inmate, employee, and visitor tracking for purposes of15follow-up investigations and vendor contract auditing. The18system must be capable of recording for such purposes the19continuous uninterrupted movement of all monitored18individuals, including those in close proximity to any19selected individual, by specific position, not by area or20zone. Such historical information must also be capable of21being archived by means of electronic data transfer to a22permanent.23b. In addition, data collected from each facility each24b. In addition, data collected from each facility each25day shall be electronically transmitted to an offsite central26clearinghouse designated by the department where the data27shall be maintained in a secure storage location in a28permanent storage medium designated as acceptable by the29department as a supplemental backup in order to protect the30archived data from alteration and to prevent loss due to	6	2. Be capable of issuing an alarm to an internal
transmitter or within 3 seconds after violation of the established parameters for permissible movement of inmates, employees, and visitors within the facility. 3.a. Be capable of maintaining a historical storage capacity sufficient to store up to 6 months of complete inmate, employee, and visitor tracking for purposes of follow-up investigations and vendor contract auditing. The system must be capable of recording for such purposes the continuous uninterrupted movement of all monitored individuals, including those in close proximity to any selected individual, by specific position, not by area or zone. Such historical information must also be capable of being archived by means of electronic data transfer to a permanent storage medium designated as acceptable by the department. b. In addition, data collected from each facility each day shall be electronically transmitted to an offsite central clearinghouse designated by the department where the data shall be maintained in a secure storage location in a permanent storage medium designated as acceptable by the department as a supplemental backup in order to protect the archived data from alteration and to prevent loss due to	7	correctional monitoring station within 3 seconds after
established parameters for permissible movement of inmates, employees, and visitors within the facility. 3.a. Be capable of maintaining a historical storage capacity sufficient to store up to 6 months of complete inmate, employee, and visitor tracking for purposes of follow-up investigations and vendor contract auditing. The system must be capable of recording for such purposes the continuous uninterrupted movement of all monitored individuals, including those in close proximity to any selected individual, by specific position, not by area or zone. Such historical information must also be capable of being archived by means of electronic data transfer to a permanent storage medium designated as acceptable by the department. b. In addition, data collected from each facility each day shall be electronically transmitted to an offsite central clearinghouse designated by the department where the data shall be maintained in a secure storage location in a permanent storage medium designated as acceptable by the department as a supplemental backup in order to protect the archived data from alteration and to prevent loss due to	8	receiving a panic alert from an employee or visitor
11employees, and visitors within the facility.123.a. Be capable of maintaining a historical storage13sapacity sufficient to store up to 6 months of complete14inmate, employee, and visitor tracking for purposes of15follow-up investigations and vendor contract auditing. The18system must be capable of recording for such purposes the17continuous uninterrupted movement of all monitored18individuals, including those in close proximity to any19selected individual, by specific position, not by area or20zone. Such historical information must also be capable of21being archived by means of electronic data transfer to a22permanent storage medium designated as acceptable by the23department.24b. In addition, data collected from each facility each25shall be electronically transmitted to an offsite central26clearinghouse designated by the department where the data27shall be maintained in a secure storage location in a28permanent storage medium designated as acceptable by the29department as a supplemental backup in order to protect the30archived data from alteration and to prevent loss due to	9	transmitter or within 3 seconds after violation of the
123.a. Be capable of maintaining a historical storage13capacity sufficient to store up to 6 months of complete14inmate, employee, and visitor tracking for purposes of15follow-up investigations and vendor contract auditing. The16system must be capable of recording for such purposes the17continuous uninterrupted movement of all monitored18individuals, including those in close proximity to any19selected individual, by specific position, not by area or20zone. Such historical information must also be capable of21being archived by means of electronic data transfer to a22permanent storage medium designated as acceptable by the23department.24b. In addition, data collected from each facility each25day shall be electronically transmitted to an offsite central26clearinghouse designated by the department where the data27shall be maintained in a secure storage location in a28permanent storage medium designated as acceptable by the29department as a supplemental backup in order to protect the29archived data from alteration and to prevent loss due to	10	established parameters for permissible movement of inmates,
13capacity sufficient to store up to 6 months of complete14inmate, employee, and visitor tracking for purposes of15follow-up investigations and vendor contract auditing. The16system must be capable of recording for such purposes the17continuous uninterrupted movement of all monitored18individuals, including those in close proximity to any19selected individual, by specific position, not by area or20zone. Such historical information must also be capable of21being archived by means of electronic data transfer to a22permanent storage medium designated as acceptable by the23department.24b. In addition, data collected from each facility each25day shall be electronically transmitted to an offsite central26clearinghouse designated by the department where the data27shall be maintained in a secure storage location in a28permanent storage medium designated as acceptable by the29department as a supplemental backup in order to protect the30archived data from alteration and to prevent loss due to	11	employees, and visitors within the facility.
Image immate, employee, and visitor tracking for purposes of14inmate, employee, and visitor tracking for purposes of15follow-up investigations and vendor contract auditing. The16system must be capable of recording for such purposes the17continuous uninterrupted movement of all monitored18individuals, including those in close proximity to any19selected individual, by specific position, not by area or20zone. Such historical information must also be capable of21being archived by means of electronic data transfer to a22permanent storage medium designated as acceptable by the23department.24b. In addition, data collected from each facility each25day shall be electronically transmitted to an offsite central26clearinghouse designated by the department where the data27shall be maintained in a secure storage location in a28permanent storage medium designated as acceptable by the29department as a supplemental backup in order to protect the30archived data from alteration and to prevent loss due to	12	3.a. Be capable of maintaining a historical storage
15follow-up investigations and vendor contract auditing. The16system must be capable of recording for such purposes the17continuous uninterrupted movement of all monitored18individuals, including those in close proximity to any19selected individual, by specific position, not by area or20zone. Such historical information must also be capable of21being archived by means of electronic data transfer to a22permanent storage medium designated as acceptable by the23department.24b. In addition, data collected from each facility each25day shall be electronically transmitted to an offsite central26clearinghouse designated by the department where the data27shall be maintained in a secure storage location in a28permanent storage medium designated as acceptable by the29department as a supplemental backup in order to protect the30archived data from alteration and to prevent loss due to	13	capacity sufficient to store up to 6 months of complete
16system must be capable of recording for such purposes the continuous uninterrupted movement of all monitored17continuous uninterrupted movement of all monitored18individuals, including those in close proximity to any19selected individual, by specific position, not by area or20zone. Such historical information must also be capable of21being archived by means of electronic data transfer to a22permanent storage medium designated as acceptable by the23department.24b. In addition, data collected from each facility each25day shall be electronically transmitted to an offsite central26clearinghouse designated by the department where the data27shall be maintained in a secure storage location in a28permanent storage medium designated as acceptable by the29department as a supplemental backup in order to protect the30archived data from alteration and to prevent loss due to	14	inmate, employee, and visitor tracking for purposes of
17continuous uninterrupted movement of all monitored18individuals, including those in close proximity to any19selected individual, by specific position, not by area or20zone. Such historical information must also be capable of21being archived by means of electronic data transfer to a22permanent storage medium designated as acceptable by the23department.24b. In addition, data collected from each facility each25day shall be electronically transmitted to an offsite central26clearinghouse designated by the department where the data27shall be maintained in a secure storage location in a28permanent storage medium designated as acceptable by the29department as a supplemental backup in order to protect the30archived data from alteration and to prevent loss due to	15	follow-up investigations and vendor contract auditing. The
 individuals, including those in close proximity to any selected individual, by specific position, not by area or zone. Such historical information must also be capable of being archived by means of electronic data transfer to a permanent storage medium designated as acceptable by the department. b. In addition, data collected from each facility each day shall be electronically transmitted to an offsite central clearinghouse designated by the department where the data shall be maintained in a secure storage location in a permanent as a supplemental backup in order to protect the archived data from alteration and to prevent loss due to 	16	system must be capable of recording for such purposes the
19 selected individual, by specific position, not by area or 20 zone. Such historical information must also be capable of 21 being archived by means of electronic data transfer to a 22 permanent storage medium designated as acceptable by the 33 department. 34 b. In addition, data collected from each facility each 45 day shall be electronically transmitted to an offsite central 56 clearinghouse designated by the department where the data 37 shall be maintained in a secure storage location in a 38 permanent storage medium designated as acceptable by the 39 department as a supplemental backup in order to protect the 30 archived data from alteration and to prevent loss due to	17	continuous uninterrupted movement of all monitored
20 zone. Such historical information must also be capable of 21 being archived by means of electronic data transfer to a 22 permanent storage medium designated as acceptable by the 33 department. 24 b. In addition, data collected from each facility each 44 day shall be electronically transmitted to an offsite central 45 day shall be electronically transmitted to an offsite central 46 clearinghouse designated by the department where the data 47 shall be maintained in a secure storage location in a 48 permanent storage medium designated as acceptable by the 49 department as a supplemental backup in order to protect the 40 archived data from alteration and to prevent loss due to	18	individuals, including those in close proximity to any
 being archived by means of electronic data transfer to a permanent storage medium designated as acceptable by the department. b. In addition, data collected from each facility each day shall be electronically transmitted to an offsite central clearinghouse designated by the department where the data shall be maintained in a secure storage location in a permanent storage medium designated as acceptable by the department as a supplemental backup in order to protect the archived data from alteration and to prevent loss due to 	19	selected individual, by specific position, not by area or
permanent storage medium designated as acceptable by the department. In addition, data collected from each facility each day shall be electronically transmitted to an offsite central clearinghouse designated by the department where the data shall be maintained in a secure storage location in a permanent storage medium designated as acceptable by the department as a supplemental backup in order to protect the archived data from alteration and to prevent loss due to	20	zone. Such historical information must also be capable of
 department. b. In addition, data collected from each facility each day shall be electronically transmitted to an offsite central clearinghouse designated by the department where the data shall be maintained in a secure storage location in a permanent storage medium designated as acceptable by the department as a supplemental backup in order to protect the archived data from alteration and to prevent loss due to 	21	being archived by means of electronic data transfer to a
 b. In addition, data collected from each facility each day shall be electronically transmitted to an offsite central clearinghouse designated by the department where the data shall be maintained in a secure storage location in a permanent storage medium designated as acceptable by the department as a supplemental backup in order to protect the archived data from alteration and to prevent loss due to 	22	permanent storage medium designated as acceptable by the
25 day shall be electronically transmitted to an offsite central 26 clearinghouse designated by the department where the data 27 shall be maintained in a secure storage location in a 28 permanent storage medium designated as acceptable by the 29 department as a supplemental backup in order to protect the 30 archived data from alteration and to prevent loss due to	23	department.
26 clearinghouse designated by the department where the data 27 shall be maintained in a secure storage location in a 28 permanent storage medium designated as acceptable by the 29 department as a supplemental backup in order to protect the 30 archived data from alteration and to prevent loss due to	24	b. In addition, data collected from each facility each
27 shall be maintained in a secure storage location in a 28 permanent storage medium designated as acceptable by the 29 department as a supplemental backup in order to protect the 30 archived data from alteration and to prevent loss due to	25	day shall be electronically transmitted to an offsite central
28 permanent storage medium designated as acceptable by the 29 department as a supplemental backup in order to protect the 30 archived data from alteration and to prevent loss due to	26	clearinghouse designated by the department where the data
29 <u>department as a supplemental backup in order to protect the</u> 30 <u>archived data from alteration and to prevent loss due to</u>	27	shall be maintained in a secure storage location in a
30 archived data from alteration and to prevent loss due to	28	permanent storage medium designated as acceptable by the
	29	department as a supplemental backup in order to protect the
31 disaster or other cause.	30	archived data from alteration and to prevent loss due to
	31	<u>disaster or other cause.</u>

13

1	4. With respect to a unit affixed to an inmate, be
2	capable of possessing an internal power source that is field
3	rechargeable or that provides a minimum of 1 year of normal
4	operation without need for recharging or replacing the power
5	source. Batteries used in units must be replaceable by
6	correctional employees. The device must emit signal content
7	that indicates the power status of the transmitter and
8	provides the correctional facility monitoring station with
9	notification of whether the power source needs to be recharged
10	or replaced.
11	5. Possess and emit signal content that indicates
12	whether the transmitter has been subjected to tampering or
13	removal.
14	6. Possess encrypted signal content or another feature
15	designed to discourage duplication.
16	7. Be of a design that is shock resistant, waterproof,
17	and capable of reliable function under normal atmospheric and
18	environmental conditions.
19	8. Be capable of wear and use in a manner that does
20	not pose a safety hazard or unduly restrict the activities of
21	the inmate.
22	9. Be capable of being attached to the inmate in a
23	manner that readily reveals any efforts to tamper with or
24	remove the transmitter upon visual inspection.
25	10. Either posses straps or other mechanisms for
26	attaching the transmitter to the inmate which are capable of
27	being adjusted to fit an inmate of any size or must be made
28	available in a variety of sizes.
29	11. Be designed and constructed in such a way as to
30	resist tampering with or removal by the inmate.
31	

1	10 Duranials a barling record source in the event of a
1	12. Provide a backup power source in the event of a
2	power failure.
3	(2) A person may not intentionally alter, tamper with,
4	damage, or destroy any electronic monitoring equipment used to
5	monitor the location of a person within a correctional
6	facility, unless the person is the owner of the equipment or
7	an agent of the owner performing ordinary maintenance and
8	repairs. A person who violates this subsection commits a
9	felony of the third degree, punishable as provided in s.
10	<u>775.082, s. 775.083, or s. 775.084.</u>
11	(3) A person may not develop, build, create, possess,
12	or use any device that is intended to mimic, clone, interfere
13	with, or jam the signal of an electronic monitoring device
14	used to monitor the location of a person within a correctional
15	facility. A person who violates this subsection commits a
16	felony of the third degree, punishable as provided in s.
17	<u>775.082, s. 775.083, or s. 775.084.</u>
18	(4) A person may not intentionally alter, tamper with,
19	damage, or destroy any data stored pursuant to subparagraph
20	(1)(c)3. unless done so with written permission from an
21	authorized official of the department or in compliance with a
22	data-retention policy of the department adopted by rule. A
23	person who violates this subsection commits a felony of the
24	third degree, punishable as provided in s. 775.082, s.
25	<u>775.083, or s. 775.084.</u>
26	(5) The department is authorized to adopt rules
27	pursuant to ss. 120.536(1) and 120.54 to implement the
28	provisions of this section.
29	Section 7. Section 985.4047, Florida Statutes, is
30	created to read:
31	
	15

1	985.4047 Electronic monitoring of juvenile offenders
2	within juvenile facilities
3	(1) The department is authorized and encouraged to
4	employ electronic monitoring of juvenile offenders within its
5	custody who are incarcerated within state and private juvenile
6	offender facilities for the purpose or reducing offender on
7	offender violence and reducing employee sexual misconduct as
8	<u>defined in s. 985.4045.</u>
9	(a) Electronic monitoring services must have the
10	capability to continuously receive and monitor electronic
11	signals from a transmitter worn by a juvenile offender so as
12	to continuously monitor an offender in real time and identify
13	at any time the offender's specific geographic position within
14	the facility. Such transmitters must update in at least
15	5-second intervals and monitor the offender's geographical
16	location to within at least a 10-foot radius of his or her
17	actual location or to within a radius that is equal to the
18	width of a facility's average size sleeping quarters,
19	whichever is less, subject to the limitations relating to the
20	state of the art of the technology used and to circumstances
21	of force majeure.
22	(b) Any electronic monitoring system employed shall
23	also provide transmitters to be worn by department employees,
24	employees of private-sector companies contracted to operate
25	juvenile facilities, and any visitors to juvenile facilities
26	who are provided access to areas that are designated for
27	authorized personnel only. Such transmitters shall include a
28	panic button and must have the capability to continuously
29	receive and monitor electronic signals from a transmitter worn
30	by an employee or visitor so as to continuously monitor
31	employees and visitors in real time and identify their

1	specific geographic positions at any time. Such transmitters
2	must update in at least 5-second intervals and monitor
3	employees and visitors to within a 10-foot radius of their
4	actual location, subject to the limitations relating to the
5	state of the art of the technology used and to circumstances
б	<u>of force majeure.</u>
7	(c) Any electronic monitoring system employed shall
8	also:
9	1. Be compatible with a commercially recognized
10	wireless network access standard as designated by the
11	department and have sufficient bandwidth to support additional
12	wireless networking devices in order to increase the capacity
13	for usage of the system by the facility.
14	2. Be capable of issuing an alarm to an internal
15	facility monitoring station within 3 seconds after receiving a
16	panic alert from an employee or visitor transmitter or within
17	3 seconds after violation of the established parameters for
18	permissible movement of offenders, employees, and visitors
19	within the facility.
20	3.a. Be capable of maintaining a historical storage
21	capacity sufficient to store up to 6 months of complete
22	offender, employee, and visitor tracking for purposes of
23	follow-up investigations and vendor contract auditing. The
24	system must be capable of recording for such purposes the
25	continuous uninterrupted movement of all monitored
26	individuals, including those in close proximity to any
27	selected individual, by specific position, not by area or
28	zone. Such historical information must also be capable of
29	being archived by means of electronic data transfer to a
30	permanent storage medium designated as acceptable by the
31	department.
	15

1	b. In addition, data collected from each facility each
2	day shall be electronically transmitted to an offsite central
3	clearinghouse designated by the department where the data
4	shall be maintained in a secure storage location in a
5	permanent storage medium designated as acceptable by the
б	department as a supplemental backup in order to protect the
7	archived data from alteration and to prevent loss due to
8	disaster or other cause.
9	4. With respect to a unit affixed to an offender, be
10	capable of possessing an internal power source that is field
11	rechargeable or that provides a minimum of 1 year of normal
12	operation without need for recharging or replacing the power
13	source and batteries must be replaceable by facility
14	employees. The device must emit signal content that indicates
15	the power status of the transmitter and provides the facility
16	monitoring station with notification of whether the power
17	source needs to be recharged or replaced.
18	5. Possess and emit signal content that indicates
19	whether the transmitter has been subjected to tampering or
20	removal.
21	6. Possess encrypted signal content or another feature
22	designed to discourage duplication.
23	7. Be of a design that is shock resistant, waterproof,
24	and capable of reliable function under normal atmospheric and
25	environmental conditions.
26	8. Be capable of wear and use in a manner that does
27	not pose a safety hazard or unduly restrict the activities of
28	the offender.
29	9. Be capable of being attached to the offender in a
30	manner that readily reveals any efforts to tamper with or
31	remove the transmitter upon visual inspection.
	18

2 <u>attaching the transmitter to the offender which are cap</u> 3 <u>being adjusted to fit an offender of any size or must k</u> 4 <u>available in a variety of sizes.</u>	
	<u>oe made</u>
4 available in a variety of gizog	
AVALIANTE III A VALLELY UL SIZES.	
5 <u>11. Be designed and constructed in such a way a</u>	<u>as to</u>
6 resist tampering with or removal by the offender.	
7 <u>12. Provide a backup power source in the event</u>	of a
8 power failure.	
9 (2) A person may not intentionally alter, tamper	r with,
10 damage, or destroy any electronic monitoring equipment	used to
11 monitor the location of a person within a juvenile faci	ility,
12 unless the person is the owner of the equipment or an a	agent of
13 the owner performing ordinary maintenance and repairs.	A
14 person who violates this subsection commits a felony of	<u>the</u>
15 third degree, punishable as provided in s. 775.082, s.	
16 <u>775.083, or s. 775.084.</u>	
17 (3) A person may not develop, build, create, pos	ssess,
18 or use any device that is intended to mimic, clone, int	<u>cerfere</u>
19 with, or jam the signal of an electronic monitoring dev	<u>vice</u>
20 used to monitor the location of a person within a juver	<u>nile</u>
21 <u>facility. A person who violates this subsection commits</u>	<u>a</u>
22 <u>felony of the third degree, punishable as provided in s</u>	<u>5.</u>
23 <u>775.082, s. 775.083, or s. 775.084.</u>	
24 (4) A person may not intentionally alter, tamper	r with,
25 damage, or destroy any data stored pursuant to subparac	graph
26 (1)(c)3. unless done so with written permission from an	
27 <u>authorized official of the department or in compliance</u>	with a
28 data-retention policy of the department adopted by rule	<u>e. A</u>
29 person who violates this subsection commits a felony of	<u>the</u>
30 third degree, punishable as provided in s. 775.082, s.	
31 <u>775.083, or s. 775.084.</u>	

Florida Senate - 2006 591-1898-06 CS for SB 450

1	(5) The department is authorized to adopt rules
2	pursuant to ss. 120.536(1) and 120.54 to implement the
3	provisions of this section.
4	Section 8. This act shall take effect October 1, 2006.
5	
6	STATEMENT OF SUBSTANTIAL CHANGES CONTAINED IN COMMITTEE SUBSTITUTE FOR
7	Senate Bill 450
8	
9 10	 Removes provisions creating probation appearance bonds to secure a defendants's appearance in future court proceedings.
11 12	 Changes offenses which bail bond agents could provide electronic monitoring for from "violent felonies" to "forcible felonies."
13	- Deletes requirement that violations of pre-trial release
14	be reported by vendors to the appropriate authorities within one hour of the offense.
15	- Removes requirement that electronic monitoring vendors pay an annual \$300 fee to the court administrator.
16 17 18	- Deletes language which would have permitted the Department of Corrections to refer certain offenders sentenced to probation or community control to bail bond agents for electronic monitoring.
19	- Adds a new Section 6 which authorizes and encourages the
20	Department of Corrections to electronically monitor inmates, employees, and some visitors in state and private correctional facilities. Sets forth
21	specifications for this equipment and provides third degree felony penalties for damaging or tampering with
22	this equipment or its stored data.
23	 Adds a new Section 7 which authorizes and encourages the Department of Juvenile Justice to electronically monitor
24	juveniles in its facilities. Establishes specifications for that equipment and provides third degree felonies for
25	damaging or tampering with the equipment or its stored data.
26	
27	
28	
29	
30	
31	