

## HOUSE OF REPRESENTATIVES STAFF FINAL BILL ANALYSIS

**BILL #:** HB 1523 Corporate Espionage  
**SPONSOR(S):** Beltran and others  
**TIED BILLS:** **IDEN./SIM. BILLS:** CS/SB 1378

---

**FINAL HOUSE FLOOR ACTION:** 115 Y's 0 N's **GOVERNOR'S ACTION:** Approved

---

### SUMMARY ANALYSIS

HB 1523 passed the House on April 14, 2021, and subsequently passed the Senate on April 26, 2021.

In general, a trade secret is a formula, process, device, or other business information that is kept confidential to maintain an advantage over competitors. Information is considered a trade secret only when it:

- Has either actual or potential independent economic value because it is not generally known;
- Is known only to a limited number of persons and has value to others who cannot legitimately access or obtain the information; and
- Is subject to reasonable measures to maintain the secrecy of the information.

Trade secret information is only protected while it remains a secret, and the information loses any available protection when independently discovered, reverse-engineered, or publicly disclosed. Because of the flexibility and broad range of information that can be protected, companies are trending more toward relying on trade secrets to protect information than traditional patent, trademark, or copyright protections. However, as the traditional workplace has evolved to provide employees greater mobility to work remotely by utilizing increased network technology and relying on data stored in "the cloud," trade secrets have become more widely targeted by both domestic and international cybercriminals seeking to profit from confidential information.

Under s. 812.081, F.S., a person commits a third degree felony if he or she:

- Deprives or withholds control of a trade secret from its owner with the intent to appropriate the trade secret to his or her own use or the use of another;
- Steals or embezzles an article representing a trade secret; or
- Makes or causes to be made a copy of an article representing a trade secret without authority.

HB 1523 creates the "Combating Corporate Espionage in Florida Act" by amending the current definitions and crimes relating to trade secret theft under s. 812.081, F.S., to modernize, simplify, and clarify what constitutes theft of a trade secret, creating the new crime of trafficking in trade secrets, and enhancing penalties under specified circumstances. Under the bill, a person commits theft of a trade secret, a third degree felony, if he or she willfully and without authorization, obtains or uses, or endeavors to obtain or use a trade secret with the intent to either temporarily or permanently:

- Deprive or withhold from its owner the control of or benefit from a trade secret; or
- Appropriate a trade secret to his or her use or to the use of another person not entitled to the trade secret.

The bill creates the crime of trafficking in trade secrets, a second degree felony, for any person who traffics in or endeavors to traffic in a trade secret he or she knows or should have known was obtained or used without authorization. If an offense under the bill is committed with the intent to benefit a foreign government, foreign agent, or foreign instrumentality, the offense is reclassified one degree higher and re-ranked one level higher on the offense severity ranking chart. The bill also requires specified restitution, provides additional civil remedies, and offers immunity from civil or criminal liability to a person who discloses a trade secret in confidence to certain authorities for investigative purposes or under seal in a legal proceeding.

The bill may have an indeterminate positive impact on the number of prison beds by creating a new felony offense and reclassifying and re-ranking offenses under certain circumstances. The bill may also allow private individuals and corporations greater ability to seek compensation in state court for stolen trade secrets.

The bill was approved by the Governor on June 7, 2021, ch. 2021-75, L.O.F., and will become effective on October 1, 2021.

This document does not reflect the intent or official position of the bill sponsor or House of Representatives.

**STORAGE NAME:** h1523z1.DOCX

**DATE:** 6/10/2021

## I. SUBSTANTIVE INFORMATION

### A. EFFECT OF CHANGES:

#### Background

Between 2002 and 2014, Amin Yu, a Chinese citizen living in Orlando as a permanent resident smuggled underwater drone parts from U.S. companies to Harbin University, a state-owned university in China conducting military research. Yu used two companies she started in the U.S. to buy systems and components for underwater vehicles under the direction of a professor at Harbin University. She then sent the parts to China, where the professor and other co-conspirators used the parts to develop drones for the Navy of the People's Liberation Army and other state entities.

In November 2018, the U.S. Department of Justice (DOJ) brought economic espionage charges against a state-owned enterprise of the People's Republic of China, a Taiwanese company, and three individuals charging them with crimes related to a conspiracy to steal, convey, and possess stolen trade secrets from a U.S. semiconductor company for the benefit of a company controlled by the Chinese government.<sup>1</sup>

In November 2019, Haitao Xiang was indicted for conspiracy to commit economic espionage, conspiracy to commit theft of trade secrets and theft of trade secrets. According to the indictment, Xiang worked as an imaging scientist for Monsanto and a subsidiary company, The Climate Corporation, from 2008 to 2017. Monsanto and The Climate Corporation developed a digital, on-line farming software platform used by farmers to collect, store, and visualize agricultural field data to increase and improve agricultural productivity. One important component of the software was a proprietary predictive algorithm referred to as the Nutrient Optimizer, which was considered a trade secret. Xiang then marketed himself to the Chinese government based on his experience, and the day after leaving his job with Monsanto and The Climate Corporation, purchased a one-way plane ticket to China. However, before he boarded his flight, Xiang was intercepted by federal officials who seized from him stolen copies of the Nutrient Optimizer.<sup>2</sup>

In February 2020, Illinois federal jurors awarded Motorola approximately \$764 million in a trade secret misappropriation and copyright infringement case against Chinese rival Hytera. The alleged misappropriation arose after a former Motorola engineer stole thousands of confidential documents and millions of lines of source code before leaving to work for Hytera, which then used the stolen information to create a competing radio.<sup>3</sup>

While approximately 80 percent of all economic espionage prosecutions brought by the DOJ allege conduct that would benefit the Chinese state,<sup>4</sup> many cases also involve U.S. companies targeting each other, for example:

- In October 2020, New York federal jurors awarded TriZetto, a healthcare information technology provider, \$855 million after finding that a competing company, Syntel, misappropriated TriZetto's trade secrets and infringed on its copyrighted software. The underlying conduct as alleged by TriZetto involved Syntel downloading hundreds of confidential

---

<sup>1</sup> U.S. Department of Justice, *PRC State-Owned Company, Taiwan Company, and Three Individuals Charged With Economic Espionage*, (Nov. 1, 2018) <https://www.justice.gov/opa/pr/prc-state-owned-company-taiwan-company-and-three-individuals-charged-economic-espionage> (last visited Apr. 28, 2021).

<sup>2</sup> U.S. Department of Justice, *Chinese National Who Worked at Monsanto Indicted on Economic Espionage Charges*, (Nov. 21, 2019) <https://www.justice.gov/opa/pr/chinese-national-who-worked-monsanto-indicted-economic-espionage-charges> (last visited Apr. 28, 2021).

<sup>3</sup> Evan M. Rothstein, Michael J. Gershoni and Bridgette C. Boyd, *United States: Trade Secret Litigation Boom Continues*, Mondaq, (Mar. 3, 2021) <https://www.mondaq.com/unitedstates/trade-secrets/1042532/trade-secret-litigation-boom-continues-> (last visited Apr. 28, 2021).

<sup>4</sup> U.S. Department of Justice, *Information About the Department of Justice's China Initiative and a Compilation of China-Related Prosecutions Since 2018*, (Feb. 11, 2021) <https://www.justice.gov/nsd/information-about-department-justice-s-china-initiative-and-compilation-china-related> (last visited Apr. 28, 2021).

key business documents, which Syntel then used to compete against TriZetto and its parent company.<sup>5</sup>

- In March 2020, a Tampa-based software solution company offering alcohol data, analytics reporting, electronic funds transfer, and payment system solutions to national retailers and distributors, Financial Information Technologies, Inc. (FINTECH), was awarded roughly \$5.7 million in a trade secret misappropriation case by the U.S. District Court for the Middle District of Florida. The verdict in the case came after a former FINTECH, employee provided stolen trade secret information to his new employer, iControl, to use in developing an electronic funds transfer payment transaction system for the beverage alcohol industry and related product suites.<sup>6</sup>

## Trade Secrets

A trade secret is generally recognized as a formula, process, device, or other business information that is kept confidential to maintain an advantage over competitors.<sup>7</sup> Information is considered a trade secret only when:

- It has either actual or potential independent economic value because it is not generally known;
- It is known only to a limited number of persons and has value to others who cannot legitimately access or obtain the information; and
- The rightful owner takes reasonable measures to maintain the secrecy of the information.<sup>8</sup>

All three elements are required for information to qualify as a trade secret, and if any element ceases to exist, the information is no longer a trade secret. As long as all three elements exist, there is no limit on the amount of time a trade secret is protected.<sup>9</sup> A wide range of valuable information is protected under trade secret law, including information that may not otherwise be protected under existing patent, trademark, or copyright law. Because a trade secret can be almost anything that provides an economic or competitive advantage to its owner, nearly every company holds trade secrets of some sort, such as a formula or recipe, a database, a business process or method, information about costs, pricing, margins, overhead, or manufacturing processes, a computer software program, a customer list, or a strategic plan.<sup>10</sup> The wide range of subject matter which may be considered a trade secret means that such information may be vital to a company's survival and often considered one of its most valuable assets.<sup>11</sup>

Unlike a copyright or patent, a trade secret may be protected in perpetuity. However, trade secret information is only protected while it remains a secret. The information loses any protection if someone else independently discovers it, reverse-engineers it, or if the trade secret is publicly disclosed.<sup>12</sup> Because of the flexibility and broad range of information that can be protected, companies are trending more toward relying on trade secrets to protect information than the traditional protections offered by a patent, trademark, or copyright.<sup>13</sup> However, as the traditional workplace has evolved to provide employees greater ability to work remotely and companies have switched from traditional information

---

<sup>5</sup> *Id.*

<sup>6</sup> *Id.*; FINTECH, *iControl Systems USA, LLC ("iControl") found guilty by jury in the U.S. District Court for the Middle District of Florida, pertaining to the theft of Fintech's trade secrets*, (Mar. 10, 2020) <https://www.fintech.com/news/fintech-llc-wins-trade-secret-theft-lawsuit-against-icontrol-systems-usa-llc/> (last visited Apr. 28, 2021).

<sup>7</sup> Black's Law Dictionary (11th ed. 2019).

<sup>8</sup> World Intellectual Property Organization, *Trade Secrets*, <https://www.wipo.int/trademarks/en/> (last visited Apr. 28, 2021).

<sup>9</sup> United States Patent and Trademark Office, *Trade Secret Policy*, (Nov. 18, 2020) <https://www.uspto.gov/ip-policy/trade-secret-policy#> (last visited Apr. 28, 2021).

<sup>10</sup> *Id.*; Michael J. Kasdan, Kevin M. Smith, and Benjamin Daniels, *Trade Secrets: What You Need to Know*, 11 National Law Review 62, 346, (Dec. 12, 2019) <https://www.natlawreview.com/article/trade-secrets-what-you-need-to-know> (last visited Apr. 28, 2021).

<sup>11</sup> *Id.*

<sup>12</sup> *Id.*

<sup>13</sup> Not only must an owner go through the lengthy process of applying for and waiting to receive a patent, trademark, or copyright, during the application process, an owner must disclose the secret itself. *Id.*

storage to an increased reliance on network technology and storing data in “the cloud,” trade secrets have become more widely targeted by cybercriminals seeking to profit from confidential information.<sup>14</sup>

## Federal Law

As the field of information technology has evolved, so have the federal laws regulating the misappropriation of proprietary information. Following the start of World War I, Congress passed the first of several laws regulating such information, the Espionage Act of 1917, which generally prohibited interfering with or attempting to undermine or interfere with the U.S. armed forces war efforts, or to in any way assist the war efforts of a U.S. war enemy. Several provisions of the Espionage Act of 1917 remain in effect and criminalize spying for or otherwise aiding an enemy of the U.S., but other provisions are expanded to punish a person who, for any reason, divulges or shares classified government information without permission.<sup>15</sup>

### *UTSA*

In an effort to clear up uncertainties and ambiguities surrounding existing trade secret laws, which often differed from state to state, the Uniform Law Commission published The Uniform Trade Secrets Act (UTSA)<sup>16</sup> in 1979 and amended it in 1985. The UTSA essentially codified the common law concerning trade secrets, but clarified the rights and remedies of trade secret owners, with the goal of standardizing trade secret law across states. As of November 2020, 48 states, including Florida, and the District of Columbia, Puerto Rico, and the U.S. Virgin Islands have enacted the UTSA.

### *EEA*

In response to an increase in foreign theft of proprietary economic information from U.S. businesses, Congress passed The Economic Espionage Act of 1996 (EEA), which was the first federal law to define<sup>17</sup> and punish the theft or misappropriation of trade secrets. The EEA criminalizes theft of trade secrets and economic espionage, as follows:

- *Theft of trade secrets* means the intentional conversion of a trade secret to the economic benefit of someone other than the owner of the trade secret, with intent or knowledge that the offense will injure the owner.<sup>18</sup>
  - Theft of trade secrets is punishable by up to 10 years in federal prison and specified fines for an individual or a corporation.<sup>19</sup>
- *Economic espionage* refers to theft of a trade secret with the intent or knowledge that such theft will benefit a foreign government, foreign instrumentality, or foreign agent.<sup>20</sup>

---

<sup>14</sup> *Id.*

<sup>15</sup> Robert Longley, *The Espionage Act of 1917: Definition, Summary, and History*, (Nov. 26, 2018) <https://www.thoughtco.com/1917-espionage-act-4177012> (last visited Apr. 28, 2021). See 18 U.S.C. ch. 37.

<sup>16</sup> A uniform act is one that seeks to establish the same law on a subject among the various jurisdictions. An act is designated as a “Uniform” Act if there is substantial reason to anticipate enactment in a large number of jurisdictions, and uniformity of the provisions of the act among the various jurisdictions is a principal objective. Uniform Law Commission, *What is a Uniform Act?* <https://www.uniformlaws.org/acts/overview/uniformacts> (last visited Apr. 28, 2021).

<sup>17</sup> Under the EEA, a trade secret means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if: the owner thereof has taken reasonable measures to keep such information secret; and the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public. 18 U.S.C. § 1839.

<sup>18</sup> 18 U.S.C. § 1832.

<sup>19</sup> An individual may be fined up to \$250,000 or twice the value of the loss or gain associated with the offense, and a corporation may be fined up to \$5 million, twice the value of the loss or gain associated with the offense, or three times the value of the stolen trade secret. 18 U.S.C. §§1832(a), 3571(c). Here and elsewhere, 18 U.S.C. § 3571(d) provides as a general matter that the maximum for a criminal fine of any federal criminal offense is the greater of the standard amount set for the particular offense (e.g., \$250,000 for individuals convicted of a felony) or twice the gain or loss resulting from the offense.

<sup>20</sup> 18 U.S.C. § 1831.

- Economic espionage is punishable by up to 15 years in federal prison and specified fines for an individual or corporation.<sup>21</sup>

The EEA requires a sentencing court to order restitution, provides that property derived from, or used to facilitate, commission of the offense may be subject to confiscation under either civil or criminal forfeiture procedures, and the court may issue an order to protect the confidentiality of a trade secret during prosecution and the government may appeal its failure to do so.

### *DTSA*

While the UTSA and EEA were effective for many years, increasing difficulty with interstate and international enforcement eventually led Congress to pass the Defend Trade Secrets Act (DTSA) of 2016,<sup>22</sup> with the goal of providing trade secret owners with a uniform, reliable, and predictable way to protect their valuable trade secrets anywhere in the country. The DTSA amended the remedies available under the EEA by establishing additional remedies for theft of a trade secret or economic espionage, including, but not limited to, the following:

- The Attorney General may sue for injunctive relief.
- A trade secret's owner may bring a private civil action for damages, equitable and injunctive, court costs, and attorney fees.
- A civil seizure mechanism is available as a preventative measure prior to a formal finding that a trade secret has been misappropriated.
- The court may require affirmative actions be taken to protect the trade secret.
- In exceptional circumstances rendering an injunction inequitable, the court may condition future use of a trade secret on payment of a reasonable royalty for no longer than the period of time for which such use could have been prohibited.<sup>23</sup>

Because the DTSA does not preempt existing state trade secret law, a trade secret owner may choose to pursue a civil action for an offense in state or federal court.

### Florida Law

Florida prohibits various acts and provides protections relating to trade secrets under both criminal and civil laws, for example:

- A person commits a third degree felony<sup>24</sup> when he or she willfully, knowingly, and without authorization discloses or takes data, a program, or supporting documentation that is a trade secret which is stored internally or externally in a computer, computer system, computer network, or electronic device.<sup>25</sup>
- A designated employee, inspector, or collaborator of the Division of Plant Industry of the Department of Agriculture and Consumer Services or the U.S. Department of Agriculture who uses his or her official capacity to obtain information that is a protected trade secret for personal gain or to reveal such information to another unauthorized person commits a first degree misdemeanor.<sup>26</sup>
- Numerous trade secrets belonging to various industries are exempt from public records.<sup>27</sup>

---

<sup>21</sup> An individual may be fined up to \$5 million or twice the value of the loss or gain associated with the offense, and a corporation may be fined up to \$10 million, twice the value of the loss or gain associated with the offense, or three times the value of the stolen trade secret. 18 U.S.C. § 1831(a).

<sup>22</sup> 18 U.S.C. § 1836.

<sup>23</sup> *Id.*

<sup>24</sup> A third degree felony is punishable by up to five years imprisonment and a \$5,000 fine. Ss. 775.082 and 775.083, F.S.

<sup>25</sup> S. 815.04, F.S.

<sup>26</sup> A first degree misdemeanor is punishable by up to one year in county jail and a \$1,000 fine Ss. 775.082 and 775.083, F.S.

<sup>27</sup> Ss. 73.0155, 73.015, 73.015, 119.0713, 215.4401, 288.075, 688.003, 688.004, 288.9626, 288.9627(2), 334.049, 395.3035(2)(c), 408.185, 408.910(14), 409.91196(1), 440.108(1), 494.00125(1)(c), 497.172(4), 501.171(11), 517.2015(1)(b), 520.9965(1)(b), 556.113(2), 559.5558(2)(b), 560.129, 569.215, 607.0505(6), 617.0503(6), 624.4212, 626.84195, 626.884(2), 627.0628(3)(g), 627.0613, 627.3518(11), 655.057, 1004.30(2), 1004.43(7), and 1004.4472, F.S.

- Florida's Uniform Trade Secrets Act<sup>28</sup> and several other statutes provide procedural safeguards and civil remedies protecting trade secrets.<sup>29</sup>

### *Theft of a Trade Secret*

Under s. 812.081, F.S., a person commits theft of a trade secret, a third degree felony, if he or she:

- Deprives or withholds control of a trade secret from its owner with the intent to appropriate the trade secret to his or her own use or the use of another;
- Steals or embezzles an article<sup>30</sup> representing<sup>31</sup> a trade secret; or
- Makes or causes to be made a copy<sup>32</sup> of an article representing a trade secret without authorization.

For purposes of committing theft of a trade secret, the term "trade secret" means the whole or any portion or phase of any formula, pattern, device, combination of devices, or compilation of information which is for use, or is used, in the operation of a business and which provides the business an advantage, or an opportunity to obtain an advantage, over others who do not know or use it.<sup>33</sup>

When a trade secret's owner takes measures to prevent the trade secret from being available to others, besides those authorized by the owner to have access for limited purposes, the trade secret is considered to be:

- Secret;
- Of value;
- For use or in use by the business; and
- Of advantage to the business, or providing an opportunity to obtain an advantage, over those who do not know or use it.<sup>34</sup>

Section 812.035, F.S., provides civil remedies for theft of a trade secret, including, but not limited to:

- Reasonable restrictions on a defendant's future activities, including prohibiting him or her from engaging in a similar endeavor used to steal the trade secret in question;
- Civil forfeiture of any property or money used in the course of or derived from the conduct in question;
- Injunctive relief, as appropriate; and
- Allowing the Department of Legal Affairs, any state attorney, or any state agency with jurisdiction to institute a civil action.<sup>35</sup>

### *Racketeering*

The Florida Racketeer Influenced and Corrupt Organization Act (RICO Act)<sup>36</sup> prohibits a person from engaging in racketeering activity. Racketeering activity means committing, attempting to commit, conspiring to commit, or soliciting, coercing, or intimidating another person to commit a listed offense,<sup>37</sup>

<sup>28</sup> Ch. 688, F.S.

<sup>29</sup> Ss. 721.071 and 812.035, F.S.

<sup>30</sup> "Article" means any object, device, machine, material, substance, or composition of matter, or any mixture or copy thereof, whether in whole or in part, including any complete or partial writing, record, recording, drawing, sample, specimen, prototype model, photograph, microorganism, blueprint, map, or copy thereof. S. 812.081(1)(a), F.S.

<sup>31</sup> "Representing" means completely or partially describing, depicting, embodying, containing, constituting, reflecting, or recording. S. 812.081(1)(b), F.S.

<sup>32</sup> "Copy" means any facsimile, replica, photograph, or other reproduction in whole or in part of an article and any note, drawing, or sketch made of or from an article or part or portion thereof. S. 812.081(1)(d), F.S.

<sup>33</sup> The term trade secret includes any scientific, technical, or commercial information, including financial information, and includes any design, process, procedure, list of suppliers, list of customers, business code, or improvement thereof. S. 812.081(1)(c), F.S.

<sup>34</sup> This applies regardless of the trade secret's novelty, invention, patentability, the state of the prior art, and the level of skill in the business, art, or field to which the subject matter pertains. *Id.*

<sup>35</sup> S. 812.035, F.S.

<sup>36</sup> Ch. 895, F.S.

<sup>37</sup> S. 895.02(8)(a), F.S.

including any violation of ch. 812, relating to theft, robbery, and related crimes, including theft of trade secrets.<sup>38</sup> Racketeering is a first degree felony, punishable by up to 30 years imprisonment and a \$10,000 fine.<sup>39</sup>

In addition to criminal penalties, the RICO Act also imposes civil liability for a violation including forfeiture to the state of all property, including money, used in the course of, intended for use in the course of, derived from, or realized through racketeering conduct.<sup>40</sup> The RICO Act also provides for specified restitution and civil penalties, authorizes a violation to be prosecuted by the Office of the Statewide Prosecutor, and allows an investigating agency to seek confidential subpoenas when the agency has reason to believe that a person or other enterprise has engaged in, or is engaging in, a violation.

## **Effect of the Bill**

HB 1523 creates the “Combating Corporate Espionage in Florida Act” by amending s. 812.081, F.S., to more closely mirror federal law by clarifying and strengthening current prohibitions against theft of trade secrets, creating the new offense of trafficking in trade secrets, and applying enhanced penalties for corporate espionage intended to benefit a foreign government.

## Definitions

The bill modernizes and simplifies relevant definitions in the following manner:

- Removes the definition and use of the terms "article," "representing," and "copy" and amends the definition of “trade secret” to include a tangible or intangible trade secret, regardless of whether or how it is stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing, to ensure that information not contained within or on a tangible article, such as information stored in “the cloud,” is captured in the definition.
- Defines “obtains or uses” and “traffic” as provided in s. 812.012, F.S., relating to theft.
- Defines “person” as a natural person, corporation, business trust, estate, trust, partnership, association, joint venture, government, governmental subdivision or agency, or any other legal or commercial entity.

## Theft of a Trade Secret

The bill updates the current crime by deleting references to "articles" and a physical "copy." Under the bill, a person commits theft of a trade secret if he or she willfully and without authorization, obtains or uses, or endeavors to obtain or use a trade secret with the intent to either temporarily or permanently:

- Deprive or withhold from its owner the control of or benefit from a trade secret; or
- Appropriately a trade secret to his or her use or to the use of another person not entitled to the trade secret.

The bill defines “obtains or uses” as any manner of:

- Taking or exercising control over property;
- Making any unauthorized use, disposition, or transfer of property;
- Obtaining property by fraud, willful misrepresentation of a future act, or false promise; or
- Conduct previously known as stealing; larceny; purloining; abstracting; embezzlement; misapplication; misappropriation; conversion; obtaining money or property by false pretenses, fraud, or deception; or other conduct similar in nature.

---

<sup>38</sup> S. 895.02(8)(a)32., F.S.

<sup>39</sup> Ss. 775.082 and 775.083, F.S.

<sup>40</sup> S. 895.05(2), F.S.

Under the bill, theft of a trade secret is a third degree felony, ranked on Level 3 of the offense severity ranking chart.<sup>41</sup>

### Trafficking in Trade Secrets

The bill creates the crime of trafficking in trade secrets to penalize any person who traffics in or endeavors to traffic in a trade secret he or she knows or should have known was obtained or used without authorization. "Endeavor" means to attempt or to try and "traffic" means:

- To sell, transfer, distribute, dispense, or otherwise dispose of property; or
- To buy, receive, possess, obtain control of, or use property with the intent to sell, transfer, distribute, dispense, or otherwise dispose of such property.

Under the bill, trafficking in trade secrets is a second degree felony, ranked on Level 5 of the offense severity ranking chart.

### Benefiting a Foreign Government

The bill provides an enhanced penalty if a person commits theft of a trade secret or trafficking in trade secrets with the intent to benefit a foreign government, foreign agent, or foreign instrumentality. The offense is reclassified one degree higher and re-ranked one level higher on the offense severity ranking chart.

"Foreign agent" means any officer, employee, proxy, servant, delegate, or representative of a foreign government and "foreign instrumentality" means any agency, bureau, ministry, component, institution, association, or any legal, commercial, or business organization, corporation, firm, or entity that is substantially owned, controlled, sponsored, commanded, managed, or dominated by a foreign government.

### Other Remedies

The bill provides the following additional remedies to more closely align with those available to a victim of trade secret crimes in federal court:

- A court must order restitution for any violation of the Act, which may include the value of the benefit received by the offender and any expenses associated with the research and design or other costs of reproducing the trade secret which the offender avoided by committing the crime.
- A court may issue an injunction prohibiting the continued improper use of a trade secret, require affirmative actions to protect the trade secret, or require payment of a reasonable royalty for future use of the trade secret for no longer than the period of time for which the improper use could have been prohibited.

Because crimes listed in ch. 812, F.S., are authorized for prosecution under the RICO Act, if an offense of theft of a trade secret or trafficking in trade secrets meets RICO Act criteria, either offense may be prosecuted under the RICO Act which authorizes heightened criminal penalties and additional civil remedies, such as forfeiture of any information or money derived from the offense.

### Exceptions

The bill provides that a person disclosing a trade secret is immune from criminal or civil liability if he or she discloses the trade secret:

---

<sup>41</sup> Felony offenses subject to the Criminal Punishment Code are listed in a single offense severity ranking chart, which uses 10 offense levels to rank felonies from least severe (Level 1) to most severe (Level 10). Each felony offense is assigned to a level according to the severity of the offense, commensurate with the harm or potential for harm to the community that is caused by the offense, as determined by statute. A person's primary offense, any other current offenses, and prior convictions are scored using the points designated for the offense severity level of each offense. The final calculation, following the scoresheet formula, determines the lowest permissible sentence that the trial court may impose, absent a valid reason for departure. S. 921.0022, F.S.



- In confidence to an attorney, law enforcement officer, or other federal, state, or local government official for the purpose of reporting or investigating a suspected violation of law; or
- Under seal in a legal proceeding.

Subject to the Governor's veto powers, the effective date of this bill is October 1, 2021.

## II. FISCAL ANALYSIS & ECONOMIC IMPACT STATEMENT

### A. FISCAL IMPACT ON STATE GOVERNMENT:

1. Revenues:

None.

2. Expenditures:

The bill may have an indeterminate positive impact on the number of prison beds by creating a new felony offense and by reclassifying and re-ranking offenses under certain circumstances.

### B. FISCAL IMPACT ON LOCAL GOVERNMENTS:

1. Revenues:

None.

2. Expenditures:

None.

### C. DIRECT ECONOMIC IMPACT ON PRIVATE SECTOR:

The bill may provide private individuals and corporate entities with greater ability to seek compensation for stolen trade secrets.

### D. FISCAL COMMENTS:

None.