

HOUSE OF REPRESENTATIVES STAFF FINAL BILL ANALYSIS

BILL #: CS/CS/CS/HB 1459 Advanced Technology

SPONSOR(S): Judiciary Committee and Appropriations Committee and Commerce Committee, McFarland

TIED BILLS: CS/HB 1461 **IDEN./SIM. BILLS:**

FINAL HOUSE FLOOR ACTION: 114 Y's

0 N's

GOVERNOR'S ACTION: Approved

SUMMARY ANALYSIS

CS/CS/CS/HB 1459 passed the House on March 6, 2024, as CS/CS/SB 1680.

Artificial intelligence (AI) encompasses a large field of existing and emerging technologies, methodologies, and application areas. AI is generally thought of as computerized systems that work and react in ways commonly thought to require intelligence. The application of AI extends to areas such as natural language processing, facial recognition, and robotics. As the use of AI technologies has grown, so too have discussions of whether and how to regulate them. Potential regulatory options include a broad regulation of AI technologies that could be used across sectors, or a more targeted approach, regulating its use in particular sectors.

The bill creates s. 282.802, F.S., to establish an advisory council called the Government Technology Modernization Council to study and monitor the development and deployment of new technologies and artificial intelligence and provide an annual report including recommendations on procuring and regulating such systems to the Governor and the Legislature.

The bill creates s. 827.072, F.S., to prohibit a person from:

- Knowingly possessing, controlling, or intentionally viewing a photograph, motion picture, representation, image, data file, computer depiction, or any other presentation which, in whole or in part, he or she knows includes generated child pornography, as a third-degree felony.
- Intentionally creating generated child pornography, as a third-degree felony.

The bill amends s. 92.561, F.S., to require any property or material that constitutes generated child pornography to be maintained in a specified manner; and to prohibit a defendant from acquiring copies of generated child pornography images as part of discovery.

The bill may have an indeterminate fiscal impact on state government and the private sector. See Fiscal Comments.

The bill was approved by the Governor on April 26, 2024, ch. 2024-118, L.O.F., and will become effective on July 1, 2024.

I. SUBSTANTIVE INFORMATION

A. EFFECT OF CHANGES:

Current Situation

Artificial Intelligence

In the 1950s, a generation of scientists, mathematicians, and philosophers, including Alan Turing, conceptualized the possibility of artificial intelligence (AI). In his 1950 paper *Computing Machinery and Intelligence*, Turing discussed “how to build intelligent machines and how to test their intelligence.”¹

The term “artificial intelligence” itself was coined at the Dartmouth Summer Research Project on Artificial Intelligence, a conference held in 1956. Since 2010, there have been many advancements in AI research which have been attributed to the “availability of large datasets, improved machine learning approaches and algorithms, and more powerful computers.”²

AI encompasses a large field of existing and emerging technologies, methodologies, and application areas. AI is “generally thought of as computerized systems that work and react in ways commonly thought to require intelligence.”³ The application of AI extends to areas such as “natural language processing, facial recognition, and robotics.”⁴

Generative Artificial Intelligence

Generative AI (GenAI), which refers to “machine learning models developed through training on large volumes of data” for the purpose of generating new content, has undergone rapid advancement over the past few years.⁵

GenAI uses advanced machine learning models⁶ such as large language models and generative adversarial networks (GANs) to generate text, images, video, and computer code responses with “human-like quality” based on user prompts.⁷ Recent technological advances combined with the open availability of these tools to the public has led to widespread use.⁸

Specifically, GANs synthesize content by pitting two neural networks⁹—a generator and discriminator—against each other. “To synthesize an image of a fictional person, the generator starts with a random array of pixels and iteratively learns to synthesize a realistic face. On each iteration, the discriminator learns to distinguish the synthesized face from a corpus of real faces; if the synthesized face is distinguishable from the real faces, then the discriminator penalizes the generator. Over multiple

¹ Rockwell Anyoha, *Can Machines Think?*, Harvard University, Aug. 28, 2017, <https://sitn.hms.harvard.edu/flash/2017/history-artificial-intelligence/> (last visited Feb. 16, 2024).

² Congressional Research Service (CRS), *Artificial Intelligence: Overview, Recent Advances, and Considerations for the 118th Congress*, <https://crsreports.congress.gov/product/pdf/R/R47644> (last visited Feb. 16, 2024).

³ *Id.*

⁴ *Id.*

⁵ *Id.*; See also CRS, *Generative Artificial Intelligence: Overview, Issues, and Questions for Congress*, <https://crsreports.congress.gov/product/pdf/IF/IF12426> (last visited Feb. 16, 2024).

⁶ Advanced machine learning models are designed to understand, interpret, generate, and respond to human language in a way that is as close to human-like communication as possible. Yana Ihnatchyck, *Introduction to GenAI: What are LLM Models, and How Are They Used in GenAI?*, Data Floq (Oct. 27, 2023), <https://datafloq.com/read/introduction-gen-ai-llm-models/> (last visited Feb. 16, 2024).

⁷ CRS, *supra* note 2.; Scribble Data, *GenAI vs. LLMs vs. NLP: A Complete Guide*, <https://www.scribbledata.io/blog/genai-vs-llms-vs-nlp-a-complete-guide/> (last visited Feb. 16, 2024).

⁸ CRS, *supra* note 2.

⁹ Neural networks, a subset of machine learning, are computational models that mimic the complex functions of the human brain. The neural networks consist of interconnected nodes or neurons that process and learn from data, enabling tasks such as pattern recognition and decision making in machine learning. Geeks for Geeks, *What is a neural network?*, <https://www.geeksforgeeks.org/neural-networks-a-beginners-guide/> (last visited Feb. 16, 2024); see IBM, *What is a neural network?*, <https://www.ibm.com/topics/neural-networks> (last visited Feb. 16, 2024).

iterations, the generator learns to synthesize increasingly more realistic faces until the discriminator is unable to distinguish it from real faces.”¹⁰

Potential Benefits and Risks of Artificial Intelligence

It has been estimated that “AI technologies could increase global GDP by \$15.7 trillion, a full 14 [percent], by 2030,” with health, retail, and financial services experiencing the most growth.¹¹ The use of AI and algorithms may benefit various sectors and services by:

- **Financial sector**¹²
 - Making decision-making relating to investing, portfolio management, loan applications, mortgages, and retirement planning more efficient, less emotional, and more analytic.
 - Preventing fraud and detecting financial anomalies in large institutions.
- **Health Sector**
 - Helping diagnose and predict disease or illness.
 - Helping predict potential challenges and allocating resources to patient education, sensing, and proactive interventions to keep patients out of the hospital.
 - Creating a multifaceted and highly personalized picture of a person’s well-being.
- **Transportation Sector**
 - Developing vehicle guidance, braking, and lane-changing systems for cars, trucks, buses, and drone delivery systems.
 - Developing systems to prevent collisions with the use of cameras and sensors.
 - Providing real-time information analysis and safety measures for the development of autonomous vehicles.
- **Government Sector**
 - Helping to create smart cities and e-governance. Examples of e-governance include:
 - The George AI chatbot, a customer service virtual assistant created by the Georgia Department of Labor.
 - AI monitoring of live footage from cameras in forests and mountains for signs of smoke by western states including California, Nevada, and Oregon.
 - Helping metropolitan areas adopt systems for citizen service delivery, urban and environmental planning, energy use, and crime prevention.
- **Customer Service**¹³
 - Providing customer service to consumers through the use of chatbots and other customer service-oriented tools to increase customer engagement, resulting in increased sales opportunities with reduced costs to the business.

However, developments in AI also raise important policy, regulatory, and ethical issues. Potential risks are associated with removing humans from the decision-making process, as may be the case when AI technology becomes more advanced over time. Some potential risks include:

- **Bias**
 - Because AI algorithms are based on training data input by humans, and because the initial data collection and actual data itself is based on human choices, responses, or decisions, there is a risk that such algorithms can contain inaccuracies and bias, which may take many forms including historical, racial, or other discrimination. Additionally, ethical considerations and value choices may be embedded into algorithms.
- **Workforce Replacement**

¹⁰ Sophie Nightingale and Hany Ford, *AI-synthesized faces are indistinguishable from real faces and more trustworthy*, Proceedings of the National Academy of Sciences of the United States of America (Feb. 14, 2022), <https://www.pnas.org/doi/epdf/10.1073/pnas.2120481119> (last visited Feb. 16, 2024).

¹¹ National Conference of State Legislatures (NCSL), *Approaches to Regulating Artificial Intelligence: A Primer*, Aug. 10, 2023, <https://www.ncsl.org/technology-and-communication/approaches-to-regulating-artificial-intelligence-a-primer> (last visited Feb. 16, 2024).

¹² *Id.*; Darrell West and John Allen, *How artificial intelligence is transforming the world*, Brookings Institute, Apr. 24, 2018, <https://www.brookings.edu/articles/how-artificial-intelligence-is-transforming-the-world/> (last visited Feb. 16, 2024).

¹³ NCSL, *supra* note 11.

- Integrating AI into the workforce brings uncertainty and challenge to the labor market, e.g., concerns regarding the extent to which AI will replace jobs. Business leaders and governments may need to make significant investments in retraining and reskilling the workforce.
- **Legal Liability**
 - There are questions concerning who is legally liable when AI systems harm or discriminate against people, especially as new and emerging uses for AI platforms are developed and integrated.
- **Security Risks¹⁴**
 - AI systems present cybersecurity and national security risks, due to:
 - AI companies collecting large amounts of personal data for AI training and use.
 - The potential for bad actors to use AI to develop advanced cyberattacks, bypass security measures, and exploit vulnerabilities in various private and public systems.
 - Traditional cybersecurity risk assessment tools are generally inadequate for addressing risks associated with AI.

Efforts to Regulate Artificial Intelligence

As the use of AI technologies has grown, so too have discussions of whether and how to regulate them. Potential regulatory options include a broad regulation of AI technologies that could be used across sectors, or a more targeted approach, regulating the use of AI technologies in particular sectors.¹⁵

In 2023, 31 states introduced at least 191 bills concerning AI, with 14 bills becoming laws.¹⁶ As reported by the National Conference of State Legislatures:¹⁷

- Connecticut required the state’s Department of Administrative Services to conduct an inventory of all systems employing AI that are in use by any state agency and, beginning February 1, 2024, to perform ongoing assessments of such systems to ensure that the use of any such system does not result in unlawful discrimination or disparate impact.
- Louisiana adopted a resolution requesting its Joint Legislative Committee on Technology and Cybersecurity to study the impact of AI in operations, procurement, and policy.
- Maryland established the Industry 4.0 Technology Grant Program to assist certain small and medium-sized manufacturing enterprises with implementing new “industry 4.0” technology or related infrastructure. The definition of industry 4.0 includes AI.
- Texas, North Dakota, Puerto Rico, and West Virginia created AI advisory councils to study and monitor AI systems developed, employed, or procured by state agencies.

Additionally, the following laws were passed in previous years:

- California prohibits any person from using a bot to communicate or interact with another person online with the intent to mislead the other person about its artificial identity in order to incentivize a purchase or sale of goods or services in a commercial transaction or to influence a vote in an election.¹⁸
- Illinois requires an employer that asks applicants to record video interviews and uses an AI analysis of applicant-submitted videos to:¹⁹

¹⁴ *Id*; Bernard Marr, *The 15 Biggest Risks Of Artificial Intelligence*, Forbes, Jun. 2, 2023, <https://www.forbes.com/sites/bernardmarr/2023/06/02/the-15-biggest-risks-of-artificial-intelligence/?sh=603d66292706> (last visited Feb. 16, 2024).

¹⁵ CRS, *supra* note 2.

¹⁶ NCSL, *State of Play | An Inside Look at Artificial Intelligence Policy and State Actions*, Jan. 9, 2024, <https://www.ncsl.org/state-legislatures-news/details/state-of-play-an-inside-look-at-artificial-intelligence-policy-and-state-actions> (last visited Feb. 16, 2024).

¹⁷ NCSL, *Artificial Intelligence 2023 Legislation*, Jan. 12, 2024, <https://www.ncsl.org/technology-and-communication/artificial-intelligence-2023-legislation> (last visited Feb. 16, 2024).

¹⁸ Cal. B&P Code §§ 17940-17943.

¹⁹ 2019 IL Public Act 101-0260.

- Notify each applicant in writing before the interview that AI may be used to analyze the applicant's facial expressions and consider the applicant's fitness for the position;
- Provide each applicant with an information sheet before the interview explaining how the AI works and what characteristics it uses to evaluate applicants; and
- Obtain written consent from the applicant to be evaluated by the AI program.

While there is no broad framework for AI regulation in the United States, federal laws on AI have been enacted over the past few years to guide actions within the federal government. For example, the National Artificial Intelligence Initiative Act of 2020 establishes the American AI Initiative and provides directions for AI research, development, and evaluation activities at federal science agencies.²⁰

Globally, the European Union has proposed the Artificial Intelligence Act (AIA), which would create broad regulatory oversight for the development and use of a wide range of AI applications, with requirements varying by risk category, from banning systems with unacceptable risk to allowing free use of those with minimal or no risk.²¹ In an effort to begin implementation of the AIA, a related new rule was agreed to in December 2023, which includes requiring human oversight in creating and deploying the systems and banning indiscriminate scraping of images from the internet to create a facial recognition database.²²

Artificial Intelligence Used to Create Child Pornography

Recently, there has been an increase in AI production of child pornography. Offenders may use downloadable open source GenAI and GAN models, which can produce images quickly, to devastating effects.²³ Hidden inside the foundation of some popular AI image-generators are thousands of images of child sexual abuse, which have made it easier for offenders and AI systems to produce realistic and explicit imagery of fake children as well as transform social media photos of fully clothed children into child sexual abuse material (CSAM).²⁴

In September 2023, analysts at the Internet Watch Foundation (IWF)²⁵ found in one dark web CSAM forum, a total of 20,254 AI-generated photos posted within the prior month. The analysts spent 87.5 hours assessing 11,108 of these images. Half of the images were found to be indecent, with 564 photos showing the most severe types of abuse.²⁶

Additionally, the Stanford Internet Observatory recently found more than 3,200 images of suspected child sexual abuse in the giant AI database LAION, an index of online images and captions that's been used to train leading AI generators.²⁷

Nishant Vishwamitra, an assistant professor at the University of Texas at San Antonio who is working on the detection of deepfakes and AI-generated CSAM images online, stated that "the scale at which such images can be created is worrisome."²⁸

Child Pornography Laws

²⁰ CRS, *supra* note 2.

²¹ *Id.*; European Commission, *Regulatory Framework Proposal on Artificial Intelligence*, <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai> (last visited Feb. 16, 2024).

²² Adam Satariano, *E.U. Agrees on Landmark Artificial Intelligence Rules*, NY Times, Dec. 8, 2023, <https://www.nytimes.com/2023/12/08/technology/eu-ai-act-regulation.html> (last visited Feb. 16, 2024).

²³ Matt Burgess, *The AI-Generated Child Abuse Nightmare Is Here*, Wired, Oct. 24, 2023, <https://www.wired.com/story/generative-ai-images-child-sexual-abuse/> (last visited Feb. 16, 2024).

²⁴ Matt O'Brien and Haleluya Hadero, *Study shows AI image-generators are being trained on explicit photos of children*, PBS NewsHour, Dec. 20, 2023, <https://www.pbs.org/newshour/science/study-shows-ai-image-generators-are-being-trained-on-explicit-photos-of-children> (last visited Feb. 16, 2024).

²⁵ A nonprofit organization based in the UK that scours and removes abuse content from the web. *Supra*, note 23.

²⁶ *Id.*

²⁷ O'Brien and Hadero, *supra* note 24.

²⁸ *Id.*

Generally, the First Amendment does not protect child pornography. In *New York v. Ferber*,²⁹ the United States Supreme Court (Supreme Court) recognized that states have a compelling interest in safeguarding the physical and psychological well-being of minors and in preventing their sexual exploitation and abuse. The Supreme Court noted that it was “unlikely that visual depictions of children . . . lewdly exhibiting their genitals would often constitute an important and necessary part of a literary performance or scientific or educational work.”³⁰ Under these principles, states have criminalized possessing, distributing, and other acts involving child pornography.

Additionally, many federal courts have held that morphed child pornography, which is created when an innocent image of a child is combined with a separate, sexually explicit image, usually of an adult, is not protected expressive speech under the First Amendment.³¹ For instance, in *United States v. Bach*, the defendant was convicted of possessing morphed child pornography. The image at issue showed a young nude boy sitting in a tree, grinning, with his pelvis tilted upward, his legs opened wide, and a full erection. The photograph of a well-known child entertainer’s head had been “skillfully inserted onto the photograph of the nude boy so that the resulting image appeared to be a nude picture of the child entertainer sitting in the tree.” The defendant appealed, arguing that his conviction was invalid because the definition of morphed child pornography violated the First Amendment. The court disagreed, holding that morphed child pornography “implicate[s] the interests of real children” and creates a lasting record of an identifiable minor child seemingly engaged in sexually explicit activity.³²

In 2014, in *United States v. Anderson*,³³ the defendant was charged with distribution of morphed child pornography relating to an image in which the face of a minor female was superimposed over the face of an adult female engaging in sex with an adult male. The defendant moved to dismiss the charge, arguing that the definition of morphed child pornography was unconstitutionally overbroad. The court noted that in the image at issue “no minor was sexually abused.”³⁴ However, the court held that because such images falsely portray identifiable children engaging in sexual activity, they implicate the compelling governmental interest in protecting minors.³⁵ Using this reasoning, the court applied a strict scrutiny balancing test and held that the definition of morphed child pornography was constitutional as applied to the facts of *Anderson*.

To date, the federal statutes relating to morphed child pornography have been upheld.³⁶

Child Pornography Prevention Action of 1996

Prior to 1996, federal law criminalized a variety of acts relating to child pornography.³⁷ At that time, federal statutes described images of a minor actually engaging in sexually explicit conduct.³⁸ In 1996, Congress passed the Child Pornography Prevention Action of 1996 (CPPA),³⁹ creating a definition of “child pornography” that for the first time criminalized acts relating to virtual child pornography.

In 2002, the Supreme Court decided *Ashcroft v. Free Speech Coalition*,⁴⁰ a case in which a California

²⁹ 458 U.S. 747 (1982).

³⁰ *Id.* at 762-63.

³¹ *U.S. v. Hotaling*, 634 F.3d 725, 728 (2d Cir. 2011).

³² 400 F.3d 622, 632 (8th Cir. 2005).

³³ 759 F.3d 891 (8th Cir. 2014).

³⁴ *Id.* at 895.

³⁵ *Id.* at 896.

³⁶ *United States v. Ramos*, 685 F.3d 120, 134 (2d Cir. 2012), *cert. denied*, 133 S.Ct. 567 (2012); *see also Doe v. Boland*, 630 F.3d 491, 497 (6th Cir. 2011); *see also United States v. Hotaling*, 634 F.3d 725 (2d Cir. 2008), *cert. denied*, 132 S.Ct. 843 (2011) (citing *Bach*, the Court held that “child pornography created by digitally altering sexually explicit photographs of adults to display the face of a child is not protected expressive speech under the First Amendment.”).

³⁷ *See*, e.g., 18 USC §2252 (1994 ed.).

³⁸ *U.S. v. Hotaling*, 599 F.Supp.2d 306, 309 (N.D.N.Y. 2008); *see also* 18 USC §§ 2252 and 2256 (1994 ed.).

³⁹ Pub. L. No. 104-208.

⁴⁰ 535 U.S. 234 (2002).

trade association for the adult entertainment industry challenged the CPPA as unconstitutionally overbroad. One provision of the CPPA prohibited “any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, that is or *appears to be*, of a minor engaging in sexually explicit conduct.” This prohibition did not depend at all on how the depiction was produced and did not require the use of an image of a real child to create the depiction. The provision captured a range of depictions, referred to as “virtual child pornography,” which may include wholly computer-generated images, as well as images produced by more traditional means.⁴¹

The Supreme Court held that the speech criminalized in the challenged provision of the CPPA violated the First Amendment since it extended the federal prohibition against child pornography to sexually explicit images that **“appeared to” depict minors but were “produced without using any real children.”**⁴² The Supreme Court decided that “by prohibiting child pornography that did not depict an actual child,” the CPPA “abridged the freedom to engage in a substantial amount of lawful speech” and was therefore overbroad and unconstitutional.⁴³

Congress attempted to remedy the constitutional issues raised in *Ashcroft* by passing the Prosecutorial Remedies and Other Tools to end the Exploitation of Children Today Act (Protect Act) in 2003.⁴⁴ The Protect Act narrowed the definition of virtual child pornography in the CPPA to prohibit a visual depiction that is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct. Additionally, the Act defined “indistinguishable” to mean, when used with respect to a depiction, virtually indistinguishable, in that the depiction is such that an ordinary person viewing the depiction would conclude that the depiction is of an actual minor engaged in sexually explicit conduct. This definition does not apply to depictions that are drawings, cartoons, sculptures, or paintings depicting minors or adults.⁴⁵

Florida Law

Section 827.01, F.S., defines:

- “Child pornography” as:
 - Any image depicting a minor engaged in sexual conduct; or
 - Any image that has been created, altered, adapted, or modified by electronic, mechanical, or other means, to portray an identifiable minor engaged in sexual conduct.⁴⁶

- “Sexual conduct” as:
 - Actual or simulated⁴⁷ sexual intercourse, deviate sexual intercourse, sexual bestiality,⁴⁸ masturbation, or sadomasochistic abuse;⁴⁹
 - Actual or simulated lewd exhibition of the genitals;
 - Actual physical contact with a person’s clothed or unclothed genitals, pubic area, buttocks, or, if such person is a female, breast, with the intent to arouse or gratify the sexual desire of either party; or

⁴¹ *Ashcroft*, 535 U.S. at 241.

⁴² *Id.* at 239.

⁴³ *Id.* at 256.

⁴⁴ Pub. L. No. 108-21.

⁴⁵ 18 USC §2256(8)(B) and (11).

⁴⁶ S. 827.071(1)(b), F.S.

⁴⁷ “Simulated” means the explicit depiction of sexual conduct which creates the appearance of such conduct and which exhibits any uncovered portion of the breasts, genitals, or buttocks. S. 827.071(1)(n), F.S.

⁴⁸ “Sexual bestiality” means any sexual act between a person and an animal involving the sex organ of the one and the mouth, anus, or female genitals of the other. S. 827.071(1)(k), F.S.

⁴⁹ “Sadomasochistic abuse” means flagellation or torture by or upon a person, or the condition of being fettered, bound, or otherwise physically restrained, for the purpose of deriving sexual satisfaction from inflicting harm on another or receiving such harm oneself. S. 827.071(1)(i), F.S.

- Any act or conduct which constitutes sexual battery⁵⁰ or simulates that sexual battery is being or will be committed.^{51, 52}
- “Identifiable minor” as a person:
 - Who was a minor at the time the image was created, altered, adapted, or modified, or whose image as a minor was used in the creating, altering, adapting, or modifying of the image; and
 - Who is recognizable as an actual person by the person’s face, likeness, or other distinguishing characteristic, such as a unique birthmark, or other recognizable feature.^{53, 54}

Florida law contains a variety of provisions prohibiting acts relating to child pornography, including:

- Section 827.071(4), F.S., which prohibits a person from possessing with the intent to promote any photograph, motion picture, exhibition, show, representation, or other presentation which, in whole or in part, includes child pornography, as a second-degree felony. Possession of three or more copies of such photographs, etc., is prima facie evidence of a person’s intent to promote.
- Section 827.071(5), F.S., which prohibits a person from knowingly possessing, controlling, or intentionally viewing⁵⁵ a photograph, motion picture, or other image that, in whole or in part, he or she knows includes any child pornography, as a third-degree felony.⁵⁶
- Section 847.0137, F.S., which prohibits a person from knowingly, or under circumstances when he or she reasonably should have known, transmitting child pornography to another person, as a third-degree felony.

While the definition of “child pornography” in Florida law currently captures morphed child pornography, it does not capture virtual child pornography. As such, Florida law does not currently prohibit the production, possession, control, intentional viewing, promotion, or transmission of an image that, although not containing or being derived from an image of a real minor, is indistinguishable from an image of a real minor engaging in sexual conduct.

Advisory Councils

Section 20.03, F.S., defines an “advisory council” as an advisory body created by specific statutory enactment and appointed to function on a continuing basis. Generally, an advisory council is enacted to study the problems arising in a specified functional or program area of state government and to provide recommendations and policy alternatives.⁵⁷

The Code of Ethics for Public Officers and Employees⁵⁸ establishes ethical standards for public officials, which includes any person elected or appointed to hold office in any agency and any person serving on an advisory council.⁵⁹ The code is intended to ensure that public officials conduct themselves independently and impartially, and do not use their offices for private gain other than

⁵⁰ “Sexual battery” means oral, anal, or female genital penetration by, or union with, the sexual organ of another or the anal or female genital penetration of another by any other object; however, “sexual battery” does not include an act done for a bona fide medical purpose. S. 827.071(1)(j), F.S.

⁵¹ S. 827.071(1)(l), F.S.

⁵² A mother’s breastfeeding of her baby does not under any circumstance constitute “sexual conduct.” *Id.*

⁵³ S. 827.071(1)(e), F.S.

⁵⁴ The term may not be construed to require proof of the actual identity of the identifiable minor. *Id.*

⁵⁵ “Intentionally view” means to deliberately, purposefully, and voluntarily view. Proof of intentional viewing requires establishing more than a single image, motion picture, exhibition, show, image, data, computer depiction, representation, or other presentation was viewed over any period of time. S. 827.071(1)(b), F.S.

⁵⁶ The statute also specifies that the possession, control, or intentional viewing of each such photograph, or other image, is a separate offense. If such photograph or other image includes child pornography depicting more than one child, then each child in each photograph or image that is knowingly possessed, controlled, or intentionally viewed is a separate offense.

⁵⁷ S. 20.03(7), F.S.; *See also* s. 20.052, F.S.

⁵⁸ *See* Part III, Chapter 112, F.S.

⁵⁹ S. 112.313(1), F.S.

compensation provided by law. The code pertains to various ethical issues, such as ethics trainings, voting conflicts, full and public disclosure of financial interests, and standards of conduct.⁶⁰

Florida Cybersecurity Advisory Council

The Department of Management Services (DMS) oversees information technology (IT)⁶¹ governance and security for the executive branch in Florida.⁶² The Florida Digital Service (FLDS) is housed within DMS and was established in 2020 to replace the Division of State Technology.⁶³ FLDS works under DMS to implement policies for IT and cybersecurity for state agencies.⁶⁴

The Florida Cybersecurity Advisory Council (CAC) is an advisory council within DMS.⁶⁵ The purpose of the CAC is to assist state agencies in protecting IT resources from cybersecurity threats and incidents and advise counties and municipalities on cybersecurity.⁶⁶ The CAC must assist FLDS in implementing best cybersecurity practices.⁶⁷ The CAC meets at least quarterly to:

- Review existing state agency cybersecurity policies;
- Assess ongoing risks to state agency IT;
- Recommend a reporting and information sharing system to notify state agencies of new risks;
- Recommend data breach simulation exercises;
- Assist FLDS in developing cybersecurity best practice recommendations;
- Examine inconsistencies between state and federal law regarding cybersecurity;
- Review information relating to cybersecurity incidents and ransomware incidents to determine commonalities and develop best practice recommendations for state agencies, counties, and municipalities; and
- Recommend any additional information that a county or municipality should report to the FLDS as part of its cybersecurity incident or ransomware incident notification under s. 282.3185, F.S.⁶⁸

The CAC must work with the National Institute of Standards and Technology⁶⁹ and other federal agencies, private sector businesses, and private cybersecurity experts to identify which local infrastructure sectors, not covered by federal law, are at the greatest risk of cyber-attacks and need the most enhanced cybersecurity measures and to identify categories of critical infrastructure as critical cyber infrastructure if cyber damage to the infrastructure could result in catastrophic consequences.⁷⁰

The CAC must also prepare and submit a comprehensive report to the Governor, the President of the Senate, and the Speaker of the House of Representatives that includes data, trends, analysis, findings, and recommendations for state and local action regarding ransomware incidents, including:

- Descriptive statistics including the amount of ransom requested, the duration of the ransomware incident, and the overall monetary cost to taxpayers of the ransomware incident.

⁶⁰ See Part III, Chapter 112, F.S.

⁶¹ The term “information technology” means equipment, hardware, software, firmware, programs, systems, networks, infrastructure, media, and related material used to automatically, electronically, and wirelessly collect, receive, access, transmit, display, store, record, retrieve, analyze, evaluate, process, classify, manipulate, manage, assimilate, control, communicate, exchange, convert, converge, interface, switch, or disseminate information of any kind or form. S. 282.0041(19), F.S.

⁶² See s. 20.22, F.S.

⁶³ Ch. 2020-161, L.O.F.

⁶⁴ See s. 20.22(2)(b), F.S.

⁶⁵ S. 282.319(1), F.S.

⁶⁶ S. 282.319(2), F.S.

⁶⁷ S. 282.319(3), F.S.

⁶⁸ S. 282.319(9), F.S.

⁶⁹ The National Institute of Standards and Technology (NIST) is a non-regulatory federal agency housed within the United States Department of Commerce. NIST’s role is to facilitate and support the development of cybersecurity risk frameworks. NIST is charged with providing a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls that may be voluntarily adopted by owners and operators of critical infrastructure to help them identify, assess, and manage cyber risks. NIST, *NIST General Information*, <https://www.nist.gov/director/pao/nist-general-information> (last visited Feb. 16, 2024); NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, p. 1, <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf> (last visited Feb. 16, 2024).

⁷⁰ S. 282.319(10), F.S.

- A detailed statistical analysis of the circumstances that led to the ransomware incident which does not include the name of the state agency, county, or municipality; network information; or system identifying information.
- A detailed statistical analysis of the level of cybersecurity employee training and frequency of data backup for the state agency, county, or municipality that reported the ransomware incident.
- Specific issues identified with current policies, procedures, rules, or statutes and recommendations to address such issues.
- Any other recommendations to prevent ransomware incidents.

Effect of Proposed Changes

Government Technology Modernization Council

The bill creates s. 282.802, F.S., to establish the Government Technology Modernization Council (council) to serve as an advisory council within DMS.

The bill provides that the purpose of the council is to study and monitor the development and deployment of new technologies and provide reports on recommendations for procurement and regulation of such systems to the Governor and the Legislature.

The bill requires the council to meet at least quarterly to:

- Recommend legislative and administrative actions that the Legislature and state agencies may take to promote the development of data modernization in Florida.
- Assess and provide guidance on necessary legislative reforms and the creation of a state code of ethics for AI systems in state government.
- Assess the effect of automated decision systems or identity management on constitutional and other legal rights, duties, and privileges of residents of this state.
- Evaluate common standards for AI safety and security measures, including the benefits of requiring disclosure of the digital provenance for all images and audio created using generative AI as a means of revealing the origin and edit of the image or audio, as well as the best methods for such disclosure.
- Assess the manner in which governmental entities and the private sector are using AI with a focus on opportunity areas for deployments in systems across this state.
- Determine the manner in which AI is being exploited by bad actors, including foreign countries of concern.⁷¹
- Evaluate the need for curriculum to prepare school-age audiences with the digital media and visual literacy skills needed to navigate the digital information landscape.

The bill requires the council to annually submit any legislative recommendations it considers necessary to modernize government technology to the Governor, the President of the Senate, and the Speaker of the House of Representatives beginning December 31, 2024. The bill requires such recommendations to include any information the council considers relevant, including policies necessary to:

- Accelerate adoption of technologies that will increase productivity of state enterprise information technology systems, improve customer service levels of government, and reduce administrative or operating costs.
- Promote the development and deployment of AI systems, financial technology, education technology, or other enterprise management software in Florida.
- Protect Floridians from bad actors who use AI.

The bill requires the council to be composed of the following members:

- The Lieutenant Governor as chair.

⁷¹ Section 287.138(1), F.S., lists the following countries as foreign countries of concern: the People's Republic of China, the Russian Federation, the Islamic Republic of Iran, the Democratic People's Republic of Korea, the Republic of Cuba, the Venezuelan regime of Nicolás Maduro, and the Syrian Arab Republic.

- The state chief information officer.
- The Secretary of Commerce or his or her designee.
- The Secretary of Health Care Administration or his or her designee.
- The Secretary of Transportation or his or her designee.
- The Executive Director of the Department of Law Enforcement or his or her designee.
- Five representatives with senior level experience or expertise in AI, cloud computing, identity management, data science, machine learning, government procurement, financial technology, educational technology, and constitutional law, with three appointed by the Governor, one appointed by the President of the Senate, and one appointed by the Speaker of the House of Representatives.
- One member of the Senate, appointed by the President of the Senate.
- One member of the House of Representatives, appointed by the Speaker of the House of Representatives.
- The Secretary of DMS, or his or her designee, who shall serve as the ex officio, nonvoting executive director of the council.

The bill provides that council members shall serve for terms of four years, except that sitting members of the Senate and the House of Representatives shall serve terms that correspond with their terms of office. For the purpose of providing staggered terms, the initial appointments of members made by the Governor are for terms of two years. Under the bill, a vacancy is filled for the remainder of the unexpired term in the same manner as the initial appointment. All members of the council are eligible for reappointment.

The bill provides that members of the council shall serve without compensation, but are entitled to receive reimbursement for per diem and travel expenses.⁷²

Child Pornography

The bill creates s. 827.072, F.S., to prohibit a person from:

- Knowingly possessing, controlling, or intentionally viewing a photograph, motion picture, representation, image, data file, computer depiction, or any other presentation which, in whole or in part, he or she knows includes generated child pornography, as a third-degree felony.
 - The bill provides that possession, control, or intentional viewing of each such photograph, motion picture, representation, image, data file, computer depiction, or other presentation is a separate offense.
- Intentionally creating generated child pornography, as a third-degree felony.

The bill defines “generated child pornography” to mean any image that has been created, altered, adapted, or modified by electronic, mechanical, or other computer-generated means to portray a fictitious person, who a reasonable person would regard as being a real person younger than 18 years of age, engaged in sexual conduct.

The bill specifies that possession, control, or intentional viewing of generated child pornography as a part of a law enforcement investigation is not prohibited under s. 827.072, F.S.

The bill amends s. 92.561, to:

- Require any property or material that constitutes generated child pornography as defined in s. 827.072, F.S., to remain secured or locked in the care, custody, and control of a law enforcement agency, the state attorney, or the court.
- Prohibit a defendant from acquiring reproductions of any kind of any property or material that constitutes generated child pornography images as part of discovery, as long as the state attorney makes the property or material available to the defendant.

⁷² As allowed under s. 112.061, F.S.

The bill provides an effective date of July 1, 2024.

II. FISCAL ANALYSIS & ECONOMIC IMPACT STATEMENT

A. FISCAL IMPACT ON STATE GOVERNMENT:

1. Revenues:

None.

2. Expenditures:

See Fiscal Comments.

B. FISCAL IMPACT ON LOCAL GOVERNMENTS:

1. Revenues:

None.

2. Expenditures:

See Fiscal Comments.

C. DIRECT ECONOMIC IMPACT ON PRIVATE SECTOR:

None.

D. FISCAL COMMENTS:

The bill may have an indeterminate positive impact on jail and prison beds by creating new felony offenses related to generated child pornography, which may result in more jail and prison admissions.

Based on the provisions of the bill, DMS will likely incur the following recurring costs that can be absorbed by existing resources:

1. Administrative support staff.
2. AI subject matter experts.
3. Travel expenses for council members and administration staff.
4. Policy analyst staff for drafting annual legislative recommendations.