STATE OF FLORIDA

OFFICE OF THE GOVERNOR
EXECUTIVE ORDER NUMBER 22-216
(Strengthening Florida Cybersecurity Against Foreign Adversaries)

WHEREAS, over two centuries ago, our country's founding fathers warned us that one of our "most deadly adversaries" would be foreign powers that attempt to improperly influence our government, THE FEDERALIST NO. 68 (Alexander Hamilton); George Washington, Farewell Address (Sept. 19, 1796), and their prescient warnings ring as true today as they ever did; and

WHEREAS, the Office of the Director of National Intelligence (ODNI) earlier this year stated that "China presents the broadest, most active, and persistent cyber espionage threat to U.S. Government and private sector networks." ODNI, Annual Threat Assessment of the U.S. Intelligence Community 8 (Feb. 2022); and

WHEREAS, ODNI further assessed that "China almost certainly is capable of launching cyber attacks that would disrupt critical infrastructure services within the United States." *Id.*; and

WHEREAS, the Chinese government has positioned itself to engage in malicious activity using technology by acquiring shares in foreign "trusted suppliers and vendors" so that the Chinese government can influence company operations; by compelling foreign companies to develop or manufacture technology components in China or to house data on servers in China; by placing government officials in high-ranking positions at companies; and by requiring companies operating in China to give the Chinese government full access to buildings and digital information, including data stored on servers, source code, encryption, and other crucial information; and

WHEREAS, ODNI further identified Russia, Iran, and North Korea as having the capability and desire to launch cyber attacks against the United States. Annual Threat Assessment of the U.S. Intelligence Community 12, 15, 17 (Feb. 2022); and

WHEREAS, the Department of Commerce promulgated an interim final rule in January 2021 that contained a list of "foreign adversaries," including the countries named above, plus Cuba and Venezuelan dictator Nicolas Maduro, and that authorized the Commerce Secretary to review certain transactions between U.S. and foreign persons that pose an undue or unacceptable risk because the contracted service or commodity is designed, developed, manufactured, or supplied by persons owned or controlled by, or subject to the jurisdiction or direction of, those foreign adversaries. Securing the Information and Communications Technology and Services Supply Chain, 86 FR 4909 (ICTS Rule); and

WHEREAS, the Department of Commerce identified the foregoing six "foreign adversaries" because they "have engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or security and safety of United States persons." ICTS Rule, 86 FR at 4914; and

WHEREAS, I signed into law section 286.101, Florida Statutes, which contains a list of "foreign countries of concern" that include all the above-mentioned countries, as well as Syria, and which requires state agencies and agencies doing business with the state to disclose certain of their dealings with those countries of concern; and

WHEREAS, article IV, section 1, subsection (a) of the Florida Constitution vests the "supreme executive power" of the State in the Governor, makes the Governor "commander-in-chief of all military forces of the state not in active service of the United States," directs the Governor to "take care that the laws be faithfully executed," and provides that the Governor "shall

be the chief administrative officer of the state responsible for the planning and budgeting for the state"; and

WHEREAS, the Legislature has, by law, provided for the protection of Floridians' intellectual property and other sensitive information, *see, e.g.*, §§ 501.171, 812.081, 815.04, .045, Florida Statutes; and

WHEREAS, the Department of Management Services (DMS), through the Florida Digital Service (collectively, "FDS"), is the lead entity responsible for modernizing state technology and information services and for determining appropriate cybersecurity measures for state agencies, *see* §§ 282.0051(1) and 282.318(3), Florida Statutes; and

WHEREAS, to achieve these ends, FDS has the authority to adopt rules pursuant to the Administrative Procedures Act and the State Cybersecurity Act; and

WHEREAS, FDS must adopt rules establishing best practices for the procurement of information technology products and cloud-computing services, *see* § 282.0051(1)(f) and (6), Florida Statutes, as well as rules governing standards necessary to facilitate a secure ecosystem of data interoperability, *see* § 282.0051(3)(d) and (6), Florida Statutes; and

WHEREAS, FDS must also adopt cybersecurity rules that mitigate risks; safeguard state agency digital assets, data, information, and information technology resources; and support a security governance framework, *see* § 282.318(3) and (10), Florida Statutes; and

WHEREAS, FDS must develop, and annually update, a statewide cybersecurity strategic plan that establishes security goals and objectives, including identification and mitigation of risks and proactive protection against threats, *see* § 282.318(3)(b), Florida Statutes; and

WHEREAS, DMS, as the primary supervisory authority over the procurement of commodities and contractual services by state agencies, may adopt rules, prescribe procedures,

and take other agency actions under the Administrative Procedures Act and Florida's procurement laws to administer the purchase of commodities and procurement of contractual services required by state agencies in Florida under chapter 287, Florida Statutes; and

WHEREAS, under section 287.042, Florida Statutes, DMS must establish a system of coordinated, uniform procurement policies, procedures, and practices to be used by state agencies in acquiring commodities and contractual services; must prescribe the methods of securing competitive sealed bids, proposals, and replies, including qualifications for vendors; must prescribe procedures for procuring information technology and consultant services that provide for public announcement and qualification, competitive solicitations, and contract award; may prescribe specific commodities and quantities that are to be purchased locally; and may establish the standards and specifications of all commodities that can be purchased by state agencies; and

WHEREAS, Florida's state and local governments face constant cyber threats that could harm Floridians, such as the well-documented attack on one of our city's water treatment facilities in 2021; and

WHEREAS, foreign adversaries seek to sabotage and corrupt key information software and systems and steal intellectual property, information on critical infrastructure, and personal information; and

WHEREAS, the technology products and services most vulnerable to malicious foreign exploitation are sold by companies that the Chinese government influences through whole or partial ownership, direct funding, or members planted in high-ranking company positions; and

WHEREAS, U.S. officials have confirmed that at least some of these technology products and services contain serious vulnerabilities, including malicious codes, capability to store critical

network credentials and other sensitive information, and preinstalled hidden hardware and software that are used by China for espionage activities; and

WHEREAS, we should do everything in our power to protect the safety and security of the State of Florida and its citizens from the exploitation of sensitive data, the disruption of critical infrastructure, and espionage activities by agents or instrumentalities of foreign countries of concern.

NOW, THEREFORE, I, RON DESANTIS, as Governor of Florida, by virtue of the authority vested in me by article IV, section 1(a) of the Florida Constitution and all other applicable laws, issue the following Executive Order to take immediate effect:

Section 1. I direct DMS to promulgate rules pursuant to section 120.54, Florida Statutes, and take any additional agency action necessary, consistent with the Constitution and laws of Florida and the United States, to ensure commodities and services used by state and local governments are not susceptible to exploitation by foreign countries of concern as defined in section 286.101, Florida Statutes, including but not limited to:

A. Preventing governmental entities in Florida from procuring or utilizing any information or communications technologies or services, components, networks, or systems that DMS has determined—after review of relevant materials, including but not limited to documentation prepared by any governmental agency, cybersecurity firm, or expert—to pose an undue or unacceptable risk to the safety and security of Florida, including because of their connection with or use by foreign countries of concern; and

B. Preventing governmental entities in Florida from procuring or utilizing any information or communications technologies or services, components, networks, or systems in similar use cases where any federal agency has prohibited, restricted the transactions

or licensing of, or otherwise limited such information or communications technologies or services, components, networks, or systems because of national security concerns; and

C. Preventing governmental entities in Florida from procuring or utilizing any information or communications technologies or services, components, networks, or systems that are designed, developed, manufactured, or supplied by companies or affiliates determined by any federal or state governmental agency to be owned, controlled by, or domiciled in a foreign country of concern, as much as feasibly possible; and

D. Preventing the exposure of governmental information and communications technologies and services, equipment, components, networks, and systems in Florida to others that are determined by any federal or state governmental agency to be owned by, controlled by, or domiciled in a foreign country of concern, as much as is feasibly possible.

When designing these rules, DMS should consider if and to what extent exceptions should exist to ensure the state does not incur losses in quality, design, workmanship, performance, or capabilities that are more detrimental to the interests of Florida than the dangers outlined in this order.

Section 2. State agencies whose agency head is appointed by and serves at the pleasure of the Governor must, to the extent possible during the rule promulgation process, ensure their current practices conform with the requirements in Section 1.

Section 3. All other state and local government entities are strongly encouraged, to the extent possible during the rule promulgation process, to conform their current practices with the requirements in Section 1.

Section 4. If any provision of this Executive Order, or the application of any provision to any person or circumstance, is held to be invalid, the remainder of this Executive Order and the application of its other provisions to any other persons or circumstances will not be affected thereby.

Section 5. This Executive Order is effective immediately.

IN TESTIMONY WHEREOF, I have hereunto set my hand and caused the Great Seal of the State of Florida to be affixed at Tallahassee, this 22nd day of September, 2022.

RON DESANTIS, GOVERNOR

ATTEST:

SECRETARY OF STATE

FILED
2022 SEP 22 PM 2:40
DEPARTMENT OF STATE
TALLAHASSEE, FL