119TH CONGRESS
1ST SESSION

S. _____

To direct the Secretary of Commerce to submit a report assessing vulnerabilities to the electric grid in the United States from certain Internet-connected devices and applications, and for other purposes.

IN THE SENATE OF THE UNITED STATES

Mr. SCOTT of Florida introduced the following bill; which was read twice and referred to the Committee on _____

A BILL

To direct the Secretary of Commerce to submit a report assessing vulnerabilities to the electric grid in the United States from certain Internet-connected devices and applications, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Preventing Remote Operations by Threatening Entities on Critical Technology for the Grid Act'' or the ''PROTECT the Grid Act''.

SEC. 2. FINDINGS; PURPOSES.

(a) FINDINGS.—Congress finds that—

(1) the rapid proliferation of high-wattage IoT devices, such as electric vehicle chargers, clothes dryers, smart air conditioners, water heaters, ovens, and similar appliances, has dramatically increased the number of connected devices in households in the United States;

(2)(A) smart appliance applications and software platforms increasingly serve as remote control interfaces; and

(B) when those applications and software platforms originate from companies operating under the jurisdiction or direction of foreign adversaries they offer a pathway for large-scale, coordinated manipulation of power demand, threatening grid stability;

(3)(A) in certain foreign adversary jurisdictions, particularly the People's Republic of China, private companies are subject to formal political oversight through mechanisms such as, in the case of the People's Republic of China, embedded Chinese Communist Party committees and executive-level Chinese Communist Party leadership; and

(B) those arrangements blur the lines between commercial activity and state-directed strategic interests;

(4) further elevating the risk to the United States electric grid is the 2017 Cybersecurity Law of the People's Republic of China (commonly referred to as the ''Chinese Cybersecurity Law''), which mandates that Chinese companies store customer data domestically and grant Chinese state authorities broad access to those data;

(5) the legal and political structures described in paragraphs (3) and (4) increase the likelihood that connected home appliances could be leveraged by foreign adversaries to target critical infrastructure in the event of a conflict with the United States;

(6) companies controlled by foreign adversaries—

(A) are actively pursuing rapid deployment of high-wattage IoT devices that could be used to attack the electric grid in the United States; and

(B) control more than 25 percent of the major appliance industry in the United States, which provides an established platform for quickly deploying those high-wattage IoT devices;

(7) through smart applications, companies controlled by foreign adversaries—

(A) are actively collecting detailed consumer data on millions of people in the United States; and

(B) have the ability to directly manipulate the demand of high-wattage devices on the electric grid;

(8) as a result, foreign adversary-controlled applications for high-wattage IoT devices create significant risk of coordinated, deliberate, demand-manipulation attacks on the electric grid in the United States;

(9) several academic studies from researchers at Princeton University, the Georgia Institute of Technology, and the University of California, Santa Cruz, point to significant risks of manipulation of demand via IoT (commonly referred to as ''MaDIoT'') attacks to manipulate power demand on the electric grid that could result in large-scale blackouts and potential damage to the electric grid;

(10) it is therefore critical to protect energy infrastructure in the United States by ensuring that smart applications embedded in home appliances are

secure and cannot serve as an entry point for foreign adversaries; and

(11) failing to address the vulnerabilities presented by those smart applications could lead to grid instability, frequency imbalances, cascading system failures, and, ultimately, catastrophic disruptions that jeopardize both public safety and the broader economy of the United States.

(b) PURPOSES.—The purposes of this Act are—

(1) to harmonize and reinforce existing national security initiatives aimed at securing the domestic information and communications technology and services (commonly referred to as ''ICTS'') supply chain against manipulation of demand, especially by the People's Republic of China; and

(2) to direct the Secretary of Commerce, in consultation with other relevant Federal officials, to submit to Congress a report containing findings and recommendations to ensure that network-connected home appliances in households in the United States do not serve as a conduit for activities by foreign adversaries or jeopardize the stability of the electric grid in the United States.

SEC. 3. DEFINITIONS.

In this Act:

(1) CONSUMER PRODUCT.—The term ''consumer product'' has the meaning given the term in section 3(a) of the Consumer Product Safety Act (15 U.S.C. 2052(a)).

(2) COVERED ENTITY.—The term ''covered entity'' means an entity that—

(A) is subject to the jurisdiction of a foreign adversary;

(B) is directly or indirectly operating on behalf of a foreign adversary; or

(C) is owned by, directly or indirectly controlled by, or otherwise subject to the direction or influence of, a foreign adversary.

(3) CRITICAL INFRASTRUCTURE.—The term ''critical infrastructure'' has the meaning given the term in subsection (e) of the Critical Infrastructures Protection Act of 2001 (42 U.S.C. 5195c).

(4) FOREIGN ADVERSARY.—The term ''foreign adversary'' means—

(A) any covered nation (as defined in section 4872(f) of title 10, United States Code); and

(B) the Bolivarian Republic of Venezuela while Nicolás Maduro Moros is in power.

(5) FOREIGN ADVERSARY-CONTROLLED APPLICATION.—The term ''foreign adversary-controlled application'' means a website, desktop application, mobile application, or augmented or immersive technology application that is operated, directly or indirectly (including through a parent, subsidiary, or affiliate (as those terms are defined in section 230.405 of title 17, Code of Federal Regulations (as in effect on the date of enactment of this Act))), by a covered entity.

(6) HIGH-WATTAGE IOT DEVICE.—The term ''high-wattage IoT device'' means any Internet-connected appliance or device that is capable of consuming or controlling electrical power at a level exceeding 500 watts, regardless of whether the device is used or designed for use in residential or commercial applications.

(7) IOT.—The term ''IoT'' means Internet of Things.

(8) RELEVANT FEDERAL OFFICIAL.—The term ''relevant Federal official'' means—

(A) any Federal official described in section 1(a) of Executive Order 13873 (84 Fed. Reg. 22689; relating to securing the information and communications technology and serv-

ices supply chain) (as in effect on the date of enactment of this Act) (or a designee of the applicable Federal official); and

(B) the head (or a designee of the head) of any other Federal department or agency that, in the determination of the Secretary of Commerce, is relevant to the purposes of this Act.

SEC. 4. REPORT ON NATIONAL SECURITY RISKS POSED BY FOREIGN ADVERSARY-CONTROLLED APPLICATIONS WITH THE CAPABILITY OF CONTROLLING HIGH-WATTAGE IOT DEVICES.

(a) IN GENERAL.—Not later than 270 days after the date of enactment of this Act, the Secretary of Commerce, in coordination with other relevant Federal officials, shall submit to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Energy and Commerce of the House of Representatives a report assessing the national security risks associated with foreign adversary-controlled applications with the ability to attack or undermine critical infrastructure in the United States.

(b) CONSIDERATIONS.—In preparing the report under subsection (a), the Secretary of Commerce shall consider, at a minimum—

(1) the extent of deployment of high-wattage IoT devices across the United States;

(2) risks relating to foreign adversary-controlled applications, especially those incorporated into consumer products that could be used to attack or otherwise destabilize the electric grid;

(3) potential impacts of those risks and any other relevant vulnerabilities on national security, including the risks of frequency imbalances, cascading failures, and other disruptions to critical infrastructure; and

(4) public comments and input from industry experts, domestic producers, importers, consumer groups, and other stakeholders regarding the security of, and the extent of foreign influence over, foreign adversary-controlled applications and high-wattage IoT devices.

(c) RECOMMENDATIONS.—The report submitted under subsection (a) shall include recommendations for mitigation measures to address any identified national security risks, which may include—

(1) an assessment of how Executive Order 13873 (84 Fed. Reg. 22689; relating to securing the information and communications technology and services supply chain) (as in effect on the date of en-

actment of this Act) may be applied to IoT devices, as such devices apply to the electric grid, to include restrictions or conditions on transactions directly involving foreign adversary-controlled applications in high-wattage IoT devices;

(2) specifically restricting the procurement by the Federal Government of consumer products with a foreign adversary-controlled application;

(3) certification or labeling requirements for high-wattage IoT devices; and

(4) any other proposal, as determined necessary by the Secretary of Commerce, in consultation with other relevant Federal officials.

SEC. 5. CODIFICATION OF EXECUTIVE ORDER 13873.

(a) IN GENERAL.—The provisions of Executive Order 13873 (84 Fed. Reg. 22689; relating to securing the information and communications technology and services supply chain) (as in effect on the date of enactment of this Act) are enacted into law.

(b) PUBLICATION.—In publishing this Act in slip form and in the United States Statutes at Large pursuant to section 112 of title 1, United States Code, the Archivist of the United States shall include after the date of approval at the end an appendix setting forth the text of

the Executive order referred to in subsection (a) (as in effect on the date of enactment of this Act).