

119TH CONGRESS
1ST SESSION

S. 2593

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

JULY 31, 2025

Mr. SCOTT of Florida introduced the following bill; which was read twice and referred to the Committee on Banking, Housing, and Urban Affairs

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.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Preventing Remote
5 Operations by Threatening Entities on Critical Tech-
6 nology for the Grid Act” or the “PROTECT the Grid
7 Act”.

1 **SEC. 2. FINDINGS; PURPOSES.**

2 (a) FINDINGS.—Congress finds that—

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

9 (2)(A) smart appliance applications and soft-
10 ware platforms increasingly serve as remote control
11 interfaces; and

12 (B) when those applications and software plat-
13 forms originate from companies operating under the
14 jurisdiction or direction of foreign adversaries they
15 offer a pathway for large-scale, coordinated manipu-
16 lation of power demand, threatening grid stability;

17 (3)(A) in certain foreign adversary jurisdictions,
18 particularly the People’s Republic of China, private
19 companies are subject to formal political oversight
20 through mechanisms such as, in the case of the Peo-
21 ple’s Republic of China, embedded Chinese Com-
22 munist Party committees and executive-level Chinese
23 Communist Party leadership; and

24 (B) those arrangements blur the lines between
25 commercial activity and state-directed strategic in-
26 terests;

1 (4) further elevating the risk to the United
2 States electric grid is the 2017 Cybersecurity Law of
3 the People’s Republic of China (commonly referred
4 to as the “Chinese Cybersecurity Law”), which man-
5 dates that Chinese companies store customer data
6 domestically and grant Chinese state authorities
7 broad access to those data;

8 (5) the legal and political structures described
9 in paragraphs (3) and (4) increase the likelihood
10 that connected home appliances could be leveraged
11 by foreign adversaries to target critical infrastruc-
12 ture in the event of a conflict with the United
13 States;

14 (6) companies controlled by foreign adver-
15 saries—

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

20 (B) control more than 25 percent of the
21 major appliance industry in the United States,
22 which provides an established platform for
23 quickly deploying those high-wattage IoT de-
24 vices;

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

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

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

4 (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;

5 (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;

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

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

3 (11) failing to address the vulnerabilities pre-
4 sented by those smart applications could lead to grid
5 instability, frequency imbalances, cascading system
6 failures, and, ultimately, catastrophic disruptions
7 that jeopardize both public safety and the broader
8 economy of the United States.

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

10 (1) to harmonize and reinforce existing national
11 security initiatives aimed at securing the domestic
12 information and communications technology and
13 services (commonly referred to as “ICTS”) supply
14 chain against manipulation of demand, especially by
15 the People’s Republic of China; and

16 (2) to direct the Secretary of Commerce, in con-
17 sultation with other relevant Federal officials, to
18 submit to Congress a report containing findings and
19 recommendations to ensure that network-connected
20 home appliances in households in the United States
21 do not serve as a conduit for activities by foreign ad-
22 versaries or jeopardize the stability of the electric
23 grid in the United States.

24 **SEC. 3. DEFINITIONS.**

25 In this Act:

1 (1) CONSUMER PRODUCT.—The term “con-
2 sumer product” has the meaning given the term in
3 section 3(a) of the Consumer Product Safety Act
4 (15 U.S.C. 2052(a)).

5 (2) COVERED ENTITY.—The term “covered en-
6 tity” means an entity that—

7 (A) is subject to the jurisdiction of a for-
8 eign adversary;

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

11 (C) is owned by, directly or indirectly con-
12 trolled by, or otherwise subject to the direction
13 or influence of, a foreign adversary.

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

18 (4) FOREIGN ADVERSARY.—The term “foreign
19 adversary” means—

20 (A) any covered nation (as defined in sec-
21 tion 4872(f) of title 10, United States Code);
22 and

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

1 (5) FOREIGN ADVERSARY-CONTROLLED APPLI-
2 CATION.—The term “foreign adversary-controlled
3 application” means a website, desktop application,
4 mobile application, or augmented or immersive tech-
5 nology application that is operated, directly or indi-
6 rectly (including through a parent, subsidiary, or af-
7 filiate (as those terms are defined in section 230.405
8 of title 17, Code of Federal Regulations (as in effect
9 on the date of enactment of this Act))), by a covered
10 entity.

11 (6) HIGH-WATTAGE IOT DEVICE.—The term
12 “high-wattage IoT device” means any Internet-con-
13 nected appliance or device that is capable of con-
14 suming or controlling electrical power at a level ex-
15 ceeding 500 watts, regardless of whether the device
16 is used or designed for use in residential or commer-
17 cial applications.

18 (7) IoT.—The term “IoT” means Internet of
19 Things.

20 (8) RELEVANT FEDERAL OFFICIAL.—The term
21 “relevant Federal official” means—

22 (A) any Federal official described in sec-
23 tion 1(a) of Executive Order 13873 (84 Fed.
24 Reg. 22689; relating to securing the informa-
25 tion 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 APPLI-
CATIONS WITH THE CAPABILITY OF CON-
TROLLING 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 (1) the extent of deployment of high-wattage
2 IoT devices across the United States;

3 (2) risks relating to foreign adversary-controlled
4 applications, especially those incorporated into con-
5 sumer products that could be used to attack or oth-
6 erwise destabilize the electric grid;

7 (3) potential impacts of those risks and any
8 other relevant vulnerabilities on national security, in-
9 cluding the risks of frequency imbalances, cascading
10 failures, and other disruptions to critical infrastruc-
11 ture; and

12 (4) public comments and input from industry
13 experts, domestic producers, importers, consumer
14 groups, and other stakeholders regarding the secu-
15 rity of, and the extent of foreign influence over, for-
16 eign adversary-controlled applications and high-watt-
17 age IoT devices.

18 (c) RECOMMENDATIONS.—The report submitted
19 under subsection (a) shall include recommendations for
20 mitigation measures to address any identified national se-
21 curity risks, which may include—

22 (1) an assessment of how Executive Order
23 13873 (84 Fed. Reg. 22689; relating to securing the
24 information and communications technology and
25 services supply chain) (as in effect on the date of en-

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

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

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

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

14 **SEC. 5. CODIFICATION OF EXECUTIVE ORDER 13873.**

15 (a) IN GENERAL.—The provisions of Executive Order
16 13873 (84 Fed. Reg. 22689; relating to securing the infor-
17 mation and communications technology and services sup-
18 ply chain) (as in effect on the date of enactment of this
19 Act) are enacted into law.

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

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

