118TH CONGRESS
2d Session
HOUSE OF REPRESENTATIVES
REPORT
118–491

COUNTERING CCP DRONES ACT

MAY 7, 2024.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mrs. RODGERS of Washington, from the Committee on Energy and Commerce, submitted the following

R E P O R T

[To accompany H.R. 2864]

The Committee on Energy and Commerce, to whom was referred the bill (H.R. 2864) to amend the Secure and Trusted Communications Networks Act of 2019 to provide for the addition of certain equipment and services produced or provided by DJI Technologies to the list of covered communications equipment or services published under such Act, and for other purposes, having considered the same, reports favorably thereon with an amendment and recommends that the bill as amended do pass.

CONTENTS

The amendment is as follows:

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the "Countering CCP Drones Act".

SEC. 2. ADDITION OF CERTAIN EQUIPMENT AND SERVICES OF DJI TECHNOLOGIES TO COVERED LIST.

(a) IN GENERAL.—Section 2(c) of the Secure and Trusted Communications Networks Act of 2019 (47 U.S.C. 1601(c)) is amended by adding at the end the following:

"(5) The communications equipment or service being—

"(A) telecommunications or video surveillance equipment produced by Shenzhen Da-Jiang Innovations Sciences and Technologies Company Limited (commonly known as 'DJI Technologies') (or any subsidiary or affiliate thereof); or

"(B) telecommunications or video surveillance services, including software, provided by an entity described in subparagraph (A) or using equipment described in such subparagraph.".

(b) CONFORMING AMENDMENTS.—Section 2 of the Secure and Trusted Communications Networks Act of 2019 (47 U.S.C. 1601) is amended by striking "paragraphs (1) through (4)" each place it appears and inserting "paragraphs (1) through (5)".

PURPOSE AND SUMMARY

H.R. 2864, the "Countering CCP Drones Act," amends the Secure and Trusted Communications Networks Act of 2019 to add telecommunications or video surveillance equipment and services produced or provided by Shenzhen Da-Jiang Innovations Sciences and Technologies Company Limited (commonly referred to as DJI Technologies, or DJI) or any subsidiary or affiliate of DJI, to the Federal Communications Commission's (FCC) covered list.

BACKGROUND AND NEED FOR LEGISLATION

The "Countering CCP Drones Act" brings into sharp focus a myriad of complex issues surrounding the utilization of Chinese-made drones, particularly those produced by DJI, the world's largest drone manufacturer. DJI's pivotal role in supplying drones to various sectors, including U.S. law enforcement agencies, has sparked heightened scrutiny about the company's ties to the Chinese government and its potential ramifications for national security and privacy.

Central to these concerns are DJI's ties to the Chinese Communist Party (CCP) and the People's Republic of China (PRC). Collectively, these government entities have significant influence and control over China-based companies, which they could use to harm the national security of the United States. For instance, the PRC's National Intelligence Law of 2017 requires PRC individuals and entities to support PRC intelligence services, including by providing data without regard to where that data was collected and without any mechanism of due process.[1] Other laws include the 2021 Data Security Law, which expands the PRC's access to and control of companies and data within China and imposes strict penalties on China-based businesses for non-compliance, and the 2021 Cyber Vulnerability Reporting Law, which requires Chinese-based companies to disclose cyber vulnerabilities found in their systems or software to PRC authorities prior to any public disclosure or sharing

[1] U.S. DEPARTMENT OF HOMELAND SECURITY, OFFICE OF STRATEGY, POLICY & PLANS, DATA SECURITY BUSINESS ADVISORY: RISKS AND CONSIDERATIONS FOR BUSINESSES USING DATA SERVICES AND EQUIPMENT FROM FIRMS LINKED TO THE PEOPLE'S REPUBLIC OF CHINA at 6 (December 22, 2020), https://www.dhs.gov/sites/default/files/publications/20_1222_data-security-business-advisory.pdf.

overseas.[2] As the ruling political party in the PRC, the CCP could use these laws to force China-based companies to share information these companies collect on Americans or to sell unsecure equipment in the United States that the CCP could exploit for cyberattacks or espionage.

DJI is subject to these laws because it is headquartered in Shenzhen, China.[3] In addition, it has received investment from the Chinese government: four investment bodies owned or administered by the CCP "have invested in [DJI] in recent years, including a state asset manager that has pledged to play a key role in promoting partnerships between private enterprises and the Chinese military."[4]

Numerous federal agencies have highlighted the threat posed by DJI drones because of the company's ties to the CCP. For example:

- The Department of Homeland Security found that "the use of Chinese-manufactured [Unmanned Aircraft Systems] in critical infrastructure operations risks exposing sensitive information to PRC authorities, jeopardizing U.S. national security, economic security, and public health and safety.";[5]
- The Department of Defense states that "systems produced by Da Jiang Innovations (DJI) pose potential threats to national security.";[6] and
- The Department of Justice (DOJ) barred the use of DOJ funds for drones made by a "Covered foreign entity . . . determined or designated, within the Department of Justice, to be subject to or vulnerable to extrajudicial direction from a foreign government," including DJI.[7]

The threat posed by DJI drones is widely known, highlighting the need to remove these drones from the U.S. communications ecosystem. Amending the Secure and Trusted Communications Networks Act to incorporate DJI's telecommunications and video surveillance equipment and services within the roster of covered communications equipment underscores a concerted endeavor to tackle these mounting apprehensions head-on.

COMMITTEE ACTION

On January 11, 2024, the Subcommittee on Communications and Technology held a hearing on cybersecurity matters. The title of the hearing was "Safeguarding Americans' Communications: Strengthening Cybersecurity in a Digital Era." The Subcommittee received testimony from:

- Jim Richberg, Head of Cyber Policy, Fortinet;
- Tobin Richardson, President and CEO, Connectivity Standards Alliance;
- Clete Johnson, Senior Fellow, Center for Strategic and International Studies; and

---

[2] https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/FINAL_NCSC_SOF_Bulletin_PRC_Laws.pdf.

[3] https://www.dji.com/company.

[4] https://www.washingtonpost.com/national-security/2022/02/01/china-funding-drones-dji-us-regulators/.

[5] https://www.cisa.gov/sites/default/files/2024-01/Cybersecurity%20Guidance%20Chinese-Manufactured%20UAS.pdf.

[6] https://www.defense.gov/News/Releases/Release/Article/2706082/department-statement-on-dji-systems/.

[7] https://www.ojp.gov/sites/g/files/xyckuh241/files/media/document/ojporderfundingdrones.pdf.

- Alan Butler, Executive Director and President, Electronic Privacy Information Center.

On February 15, 2024, the Subcommittee on Communications and Technology held a hearing on multiple bills, including H.R. 2864. The title of the hearing was "Securing Communications Networks from Foreign Adversaries." The Subcommittee received testimony from:

- James Lewis, Senior Vice President, Center for Strategic and International Studies;
- Craig Singleton, China Program Senior Director and Senior Fellow, Foundation of Defense of Democracies; and
- Lindsay Gorman, Senior Fellow for Emerging Technologies, German Marshall Fund's Alliance for Securing Democracy.

On March 12, 2024, the Subcommittee on Communications and Technology met in open markup session and forwarded H.R. 2864, as amended, to the full Committee by vote of 21 yeas and 0 nays.

On March 20, 2024, the full Committee on Energy and Commerce met in open markup session and ordered H.R. 2864, as amended, favorably reported to the House by a record vote of 43 yeas and 0 nays.

COMMITTEE VOTES

Clause 3(b) of rule XIII requires the Committee to list the record votes on the motion to report legislation and amendments thereto. The following reflects the record votes taken during the Committee consideration:

COMMITTEE ON ENERGY AND COMMERCE
118TH CONGRESS
ROLL CALL VOTE # 1

BILL: H.R. 2864, Countering CCP Drones Act

AMENDMENT: A motion by Chair Rodgers to order H.R. 2864 favorably reported to the House, as amended (Final Passage)

DISPOSITION: AGREED TO, by a roll call vote of 43 yeas to 0 nays.

REPRESENTATIVE	YEAS	NAYS	PRESENT	REPRESENTATIVE	YEAS	NAYS	PRESENT
Rep. Rodgers	X			Rep. Pallone	X		
Rep. Burgess	X			Rep. Eshoo	X		
Rep. Latta	X			Rep. DeGette	X		
Rep. Guthrie	X			Rep. Schakowsky	X		
Rep. Griffith	X			Rep. Matsui	X		
Rep. Bilirakis	X			Rep. Castor	X		
Rep. Bucshon	X			Rep. Sarbanes	X		
Rep. Hudson	X			Rep. Tonko	X		
Rep. Walberg				Rep. Clarke	X		
Rep. Carter				Rep. Cárdenas	X		
Rep. Duncan	X			Rep. Ruiz	X		
Rep. Palmer	X			Rep. Peters	X		
Rep. Dunn	X			Rep. Dingell	X		
Rep. Curtis				Rep. Veasey	X		
Rep. Lesko	X			Rep. Kuster	X		
Rep. Pence	X			Rep. Kelly			
Rep. Crenshaw	X			Rep. Barragán	X		
Rep. Joyce	X			Rep. Blunt Rochester			
Rep. Armstrong				Rep. Soto	X		
Rep. Weber	X			Rep. Craig	X		
Rep. Allen	X			Rep. Schrier	X		
Rep. Balderson	X			Rep. Trahan	X		
Rep. Fulcher	X			Rep. Fletcher	X		
Rep. Pfluger							
Rep. Harshbarger	X						
Rep. Miller-Meeks							
Rep. Cammack	X						
Rep. Obernolte	X						

03/20/2024

OVERSIGHT FINDINGS AND RECOMMENDATIONS

Pursuant to clause 2(b)(1) of rule X and clause 3(c)(1) of rule XIII, the Committee held hearings and made findings that are reflected in this report.

NEW BUDGET AUTHORITY, ENTITLEMENT AUTHORITY, AND TAX EXPENDITURES

Pursuant to clause 3(c)(2) of rule XIII, the Committee finds that H.R. 2864 would result in no new or increased budget authority, entitlement authority, or tax expenditures or revenues.

CONGRESSIONAL BUDGET OFFICE ESTIMATE

Pursuant to clause 3(c)(3) of rule XIII, at the time this report was filed, the cost estimate prepared by the Director of the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974 was not available.

FEDERAL MANDATES STATEMENT

The Committee adopts as its own the estimate of Federal mandates prepared by the Director of the Congressional Budget Office pursuant to section 423 of the Unfunded Mandates Reform Act.

STATEMENT OF GENERAL PERFORMANCE GOALS AND OBJECTIVES

Pursuant to clause 3(c)(4) of rule XIII, the general performance goal or objective of this legislation is to add communications equipment and services produced by DJI to the FCC's covered list, which would prohibit the FCC from authorizing the use of such equipment and services.

DUPLICATION OF FEDERAL PROGRAMS

Pursuant to clause 3(c)(5) of rule XIII, no provision of H.R. 2864 is known to be duplicative of another Federal program, including any program that was included in a report to Congress pursuant to section 21 of Public Law 111–139 or the most recent Catalog of Federal Domestic Assistance.

RELATED COMMITTEE AND SUBCOMMITTEE HEARINGS

Pursuant to clause 3(c)(6) of rule XIII, the following related hearings were used to develop or consider H.R. 2864:

- On January 11, 2024, the Subcommittee on Communications and Technology held a hearing on cybersecurity matters. The title of the hearing was "Safeguarding Americans' Communications: Strengthening Cybersecurity in a Digital Era." The Subcommittee received testimony from:
  - Jim Richberg, Head of Cyber Policy, Fortinet;
  - Tobin Richardson, President and CEO, Connectivity Standards Alliance;
  - Clete Johnson, Senior Fellow, Center for Strategic and International Studies; and
  - Alan Butler, Executive Director and President, Electronic Privacy Information Center.

- On February 15, 2024, the Subcommittee on Communications and Technology held a hearing on multiple bills, including H.R. 2864. The title of the hearing was "Securing Communications Networks from Foreign Adversaries." The Subcommittee received testimony from:
  - James Lewis, Senior Vice President, Center for Strategic and International Studies;
  - Craig Singleton, China Program Senior Director and Senior Fellow, Foundation of Defense of Democracies; and
  - Lindsay Gorman, Senior Fellow for Emerging Technologies, German Marshall Fund's Alliance for Securing Democracy.

COMMITTEE COST ESTIMATE

Pursuant to clause 3(d)(1) of rule XIII, at the time this report was filed, the estimate was not available.

EARMARK, LIMITED TAX BENEFITS, AND LIMITED TARIFF BENEFITS

Pursuant to clause 9(e), 9(f), and 9(g) of rule XXI, the Committee finds that H.R. 2864 contains no earmarks, limited tax benefits, or limited tariff benefits.

ADVISORY COMMITTEE STATEMENT

No advisory committees within the meaning of Section 5(b) of the Federal Advisory Committee Act were created by this legislation.

APPLICABILITY TO LEGISLATIVE BRANCH

The Committee finds that the legislation does not relate to the terms and conditions of employment or access to public services or accommodations within the meaning of section 102(b)(3) of the Congressional Accountability Act.

SECTION-BY-SECTION ANALYSIS OF THE LEGISLATION

Section 1. Short title

This section provides that the Act may be cited as the "Countering CCP Drones Act."

Section 2. Addition of certain equipment and services of DJI technologies to covered list

Subsection (a) would amend the Secure and Trusted Communications Networks Act by adding a new paragraph (5), which would add telecommunications or video surveillance equipment produced by DJI (or any subsidiary or affiliate) to the FCC's covered list. It would also add telecommunications or video surveillance services, including software, provided by DJI (or any subsidiary or affiliate) or using equipment provided by DJI (or any subsidiary or affiliate).

Subsection (b) would make conforming amendments to the Secure and Trusted Communications Networks Act by updating references from "paragraphs (1) through (4)" to "paragraphs (1) through (5)".

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italics, and existing law in which no change is proposed is shown in roman):

SECURE AND TRUSTED COMMUNICATIONS NETWORKS ACT OF 2019

* * * * * * *

SEC. 2. DETERMINATION OF COMMUNICATIONS EQUIPMENT OR SERVICES POSING NATIONAL SECURITY RISKS.

(a) PUBLICATION OF COVERED COMMUNICATIONS EQUIPMENT OR SERVICES LIST.—Not later than 1 year after the date of the enactment of this Act, the Commission shall publish on its website a list of covered communications equipment or services.

(b) PUBLICATION BY COMMISSION.—The Commission shall place on the list published under subsection (a) any communications equipment or service, if and only if such equipment or service—

(1) is produced or provided by any entity, if, based exclusively on the determinations described in [paragraphs (1) through (4)] *paragraphs (1) through (5)* of subsection (c), such equipment or service produced or provided by such entity poses an unacceptable risk to the national security of the United States or the security and safety of United States persons; and

(2) is capable of—

(A) routing or redirecting user data traffic or permitting visibility into any user data or packets that such equipment or service transmits or otherwise handles;

(B) causing the network of a provider of advanced communications service to be disrupted remotely; or

(C) otherwise posing an unacceptable risk to the national security of the United States or the security and safety of United States persons.

(c) RELIANCE ON CERTAIN DETERMINATIONS.—In taking action under subsection (b)(1), the Commission shall place on the list any communications equipment or service that poses an unacceptable risk to the national security of the United States or the security and safety of United States persons based solely on one or more of the following determinations:

(1) A specific determination made by any executive branch interagency body with appropriate national security expertise, including the Federal Acquisition Security Council established under section 1322(a) of title 41, United States Code.

(2) A specific determination made by the Department of Commerce pursuant to Executive Order No. 13873 (84 Fed. Reg. 22689; relating to securing the information and communications technology and services supply chain).

(3) The communications equipment or service being covered telecommunications equipment or services, as defined in section 889(f)(3) of the John S. McCain National Defense Author-

ization Act for Fiscal Year 2019 (Public Law 115-232; 132 Stat. 1918).

(4) A specific determination made by an appropriate national security agency.

(5) The communications equipment or service being—

(A) telecommunications or video surveillance equipment produced by Shenzhen Da-Jiang Innovations Sciences and Technologies Company Limited (commonly known as "DJI Technologies") (or any subsidiary or affiliate thereof); or

(B) telecommunications or video surveillance services, including software, provided by an entity described in subparagraph (A) or using equipment described in such subparagraph.

(d) UPDATING OF LIST.—

(1) IN GENERAL.—The Commission shall periodically update the list published under subsection (a) to address changes in the determinations described in **[**paragraphs (1) through (4)**]** *paragraphs (1) through (5)* of subsection (c).

(2) MONITORING OF DETERMINATIONS.—The Commission shall monitor the making or reversing of the determinations described in **[**paragraphs (1) through (4)**]** *paragraphs (1) through (5)* of subsection (c) in order to place additional communications equipment or services on the list published under subsection (a) or to remove communications equipment or services from such list. If a determination described in any such paragraph that provided the basis for a determination by the Commission under subsection (b)(1) with respect to any communications equipment or service is reversed, the Commission shall remove such equipment or service from such list, except that the Commission may not remove such equipment or service from such list if any other determination described in any such paragraph provides a basis for inclusion on such list by the Commission under subsection (b)(1) with respect to such equipment or service.

(3) PUBLIC NOTIFICATION.—For each 12-month period during which the list published under subsection (a) is not updated, the Commission shall notify the public that no updates were necessary during such period to protect national security or to address changes in the determinations described in **[**paragraphs (1) through (4)**]** *paragraphs (1) through (5)* of subsection (c).

* * * * * * *

○