

UNMANNED AERIAL SECURITY ACT

JULY 19, 2023.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. GREEN of Tennessee, from the Committee on Homeland Security, submitted the following

R E P O R T

[To accompany H.R. 1501]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security, to whom was referred the bill (H.R. 1501) to prohibit the Secretary of Homeland Security from operating or procuring certain foreign-made unmanned aircraft systems, and for other purposes, having considered the same, reports favorably thereon with an amendment and recommends that the bill as amended do pass.

CONTENTS

	Page
Purpose and Summary	3
Background and Need for Legislation	3
Hearings	5
Committee Consideration	6
Committee Votes	6
Committee Oversight Findings	6
C.B.O. Estimate, New Budget Authority, Entitlement Authority, and Tax Expenditures	6
Federal Mandates Statement	7
Duplicative Federal Programs	7
Statement of General Performance Goals and Objectives	7
Congressional Earmarks, Limited Tax Benefits, and Limited Tariff Benefits ...	7
Advisory Committee Statement	7
Applicability to Legislative Branch	8
Section-by-Section Analysis of the Legislation	8

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 “Unmanned Aerial Security Act” or the “UAS Act”.

SEC. 2. PROHIBITION ON OPERATION OR PROCUREMENT OF CERTAIN FOREIGN-MADE UNMANNED AIRCRAFT SYSTEMS.

(a) **PROHIBITION ON AGENCY OPERATION OR PROCUREMENT.**—Except as provided in subsection (b) and subsection (c)(3), the Secretary of Homeland Security may not operate, provide financial assistance for, or enter into or renew a contract for the procurement of—

(1) an unmanned aircraft system (UAS) that—

(A) is manufactured in a covered foreign country or by a business entity domiciled in a covered foreign country;

(B) uses flight controllers, radios, data transmission devices, cameras, or gimbals manufactured in a covered foreign country or by a business entity domiciled in a covered foreign country;

(C) uses a ground control system or operating software developed in a covered foreign country or by a business entity domiciled in a covered foreign country; or

(D) uses network connectivity or data storage located in a covered foreign country or administered by a business entity domiciled in a covered foreign country;

(2) a software operating system associated with a UAS that uses network connectivity or data storage located in a covered foreign country or administered by a business entity domiciled in a covered foreign country; or

(3) a system for the detection or identification of a UAS, which system is manufactured in a covered foreign country or by a business entity domiciled in a covered foreign country.

(b) **WAIYER.**—

(1) **IN GENERAL.**—The Secretary of Homeland Security is authorized to waive the prohibition under subsection (a) if the Secretary certifies in writing to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate that a UAS, a software operating system associated with a UAS, or a system for the detection or identification of a UAS described in any of paragraphs (1) through (3) of such subsection that is the subject of such a waiver is required—

(A) in the national interest of the United States;

(B) for counter-DAS surrogate research, testing, development, evaluation, or training; or

(C) for intelligence, electronic warfare, or information warfare operations, testing, analysis, and or training.

(2) **NOTICE.**—The certification described in paragraph (1) shall be submitted to the Committees specified in such paragraph by not later than the date that is 14 days after the date on which a waiver is issued under such paragraph.

(c) **EFFECTIVE DATES.**—

(1) **IN GENERAL.**—This Act shall take effect on the date that is 120 days after the date of the enactment of this Act.

(2) **WAIYER PROCESS.**—Not later than 60 days after the date of the enactment of this Act, the Secretary of Homeland Security shall establish a process by which the head of an office or component of the Department of Homeland Security may request a waiver under subsection (b).

(3) **EXCEPTION.**—Notwithstanding the prohibition under subsection (a), the head of an office or component of the Department of Homeland Security may continue to operate a UAS, a software operating system associated with a UAS, or a system for the detection or identification of a UAS described in any of paragraphs (1) through (3) of such subsection that was in the inventory of such office or component on the day before the effective date of this Act until—

(A) such time as the Secretary of Homeland Security has—

(i) granted a waiver relating thereto under subsection (b); or

(ii) declined to grant such a waiver; or

(B) one year after the date of the enactment of this Act, whichever is later.

(d) **DRONE ORIGIN SECURITY REPORT TO CONGRESS.**—Not later than 180 days after the date of the enactment of this Act, the Secretary of Homeland Security shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a terrorism threat assessment and report that contains information relating to the following:

(1) The extent to which the Department of Homeland Security has previously analyzed the threat that a UAS, a software operating system associated with a UAS, or a system for the detection or identification of a UAS described in any of paragraphs (1) through (3) of subsection (a) operating in the United States poses, and the results of such analysis.

(2) The number of UAS, software operating systems associated with a UAS, or systems for the detection or identification of a UAS described in any of paragraphs (1) through (3) of subsection (a) in operation by the Department, including an identification of the component or office of the Department at issue, as of such date.

(3) The extent to which information gathered by a UAS, a software operating system associated with a UAS, or a system for the detection or identification of a UAS described in any of paragraphs (1) through (3) of subsection (a) could be employed to harm the national or economic security of the United States.

(e) DEFINITIONS.—In this section:

(1) BUSINESS ENTITY.—The term “business entity” has the meaning given such term in section 334 of the Graham-Leach-Bliley Act (15 U.S.C. 6764).

(2) COVERED FOREIGN COUNTRY.—The term “covered foreign country” means a country that—

(A) the intelligence community has identified as a foreign adversary in its most recent Annual Threat Assessment; or

(B) the Secretary of Homeland Security, in coordination with the Director of National Intelligence, has identified as a foreign adversary that is not included in such Annual Threat Assessment.

(3) INTELLIGENCE COMMUNITY.—The term “intelligence community” has the meaning given such term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)).

(4) UNMANNED AIRCRAFT SYSTEM; UAS.—The terms “unmanned aircraft system” and “UAS” have the meaning given the term “unmanned aircraft system” in section 44801 of title 49, United States Code.

PURPOSE AND SUMMARY

H.R. 1501, the “Unmanned Aerial Security Act,” prohibits the Department of Homeland Security (DHS) from operating, providing financial assistance for, entering into, or renewing a contract for any unmanned aircraft systems (UAS), known as drones, that are manufactured in certain adversarial foreign countries, or by a business entity domiciled in such foreign countries. Adversarial foreign countries include those that are identified in the Office of the Director of National Intelligence’s February 2023 Annual Threat Assessment of the U.S. Intelligence Community (which includes the People’s Republic of China (PRC), Russia, Iran, and North Korea)¹ and other countries designated by DHS. H.R. 1501 also includes a waiver on the prohibition on using or purchasing UAS from covered foreign countries after certifying in writing to Congress that the UAS, is in the national interest of the United States, is needed for counter-UAS research and training, or is for intelligence and warfare information testing and analysis. Finally, an office or component of DHS may continue to use a UAS or system in its supply that would otherwise be barred until DHS grants or denies a waiver or until one year after this legislation is enacted.

BACKGROUND AND NEED FOR LEGISLATION

The need for this legislation is critical so that DHS may protect the United States against potential threats to U.S. counterintelligence efforts and critical infrastructure posed by UAS that is manufactured in foreign adversarial countries, which includes the PRC, Russia, Iran, and North Korea.² The PRC poses a particularly acute threat in this space given its domination of the global

¹Office of the Director of National Intelligence, Annual Threat Assessment of the U.S. Intelligence Committee (Feb. 6, 2023).

²Brian Harrell and Travis Moran, *The pressing threat of Chinese-made drones flying above U.S. critical infrastructure*, Cyberscoop (March 23, 2023) <https://cyberscoop.com/chinese-drone-threat-dji-regulation-critical-infrastructure/>.

UAS market.³ The PRC, led by the Chinese Communist Party, aggressively seeks to undermine the global rules-based order as well as U.S. interests through economic, political, and military power.⁴ This legislation aims to safeguard the sensitive data collected by UAS for homeland security purposes and combat the PRC's aggressions towards the United States.

DHS uses UAS for a number of important functions, including but not limited to, enhancing situational awareness at the Southwest border,⁵ conducting counter-UAS efforts in the U.S. homeland,⁶ and meeting the U.S. Coast Guard National Security Cutter's operational need for a persistent airborne surveillance capability.⁷ Unfortunately, numerous U.S. federal agencies rely on foreign-made UAS, particularly those made in the PRC.⁸ A single Chinese UAS manufacturer, DJI Technology Co., owns over 70 percent of the global market share.⁹ In June 2020, the former Cybersecurity and Infrastructure Security Agency Director wrote of DJI Technology Co. saying that "any information collected by a drone from this particular manufacturer should be considered at risk and protected from inadvertent disclosure."¹⁰ As a result of this threat, several other Departments, such as Commerce and the Interior, have taken actions to ground their drone fleets until the threat to United States government data can be determined.¹¹ DHS has also issued warnings in recent years about Chinese-made drones, specifically citing concerns that they may be sending sensitive data to their manufacturers in China, where it can then be accessed by the Chinese government.¹²

Additionally, under the PRC's National Intelligence Law, as amended in 2018, all organizations and citizens are required to support, assist, and cooperate with the PRC's intelligence work.¹³ Under this law, all Chinese organizations and citizens, to include

³Nessa Anwar, World's largest drone maker is unfazed—even if it's blacklisted by the U.S. CNBC (Feb. 7, 2023) <https://www.cnbc.com/2023/02/08/worlds-largest-drone-maker-dji-is-unfazed-by-challenges-like-us-blacklist.html>.

⁴White House, *United States Strategic Approach to the People's Republic of China* (2020) <https://trumpwhitehouse.archives.gov/wp-content/uploads/2020/05/U.S.-Strategic-Approach-to-The-Peoples-Republic-of-China-Report-5.24v1.pdf>.

⁵John Davis, *Small but Mighty: Border Patrol's use of small drones is a game changer in border security*, US CBP (last accessed May 31, 2023) <https://www.cbp.gov/frontline/cbp-small-drones-program>.

⁶U.S. Dep't of Homeland Sec., Counter-Unmanned Aircraft Systems (C-UAS) (last accessed May 31, 2023) <https://www.dhs.gov/science-and-technology/counter-unmanned-aircraft-systems-c-uas>.

⁷U.S. Dep't of Homeland Sec. USCG, Unmanned Aircraft Systems (last accessed May 31, 2023) <https://www.dcms.uscg.mil/Our-Organization/Assistant-Commandant-for-Acquisitions-CG-9/Programs/Air-Programs/UAS/>.

⁸Annie I. Antón, Olivia C. Mauger, *U.S. Reliance on Chinese Drones: A Sector for the Next CHIPS Act?* (May 25, 2023) <https://www.lawfareblog.com/us-reliance-chinese-drones-sector-next-chips-act>.

⁹Nessa Anwar, World's largest drone maker is unfazed—even if it's blacklisted by the U.S. CNBC (Feb. 7, 2023) <https://www.cnbc.com/2023/02/08/worlds-largest-drone-maker-dji-is-unfazed-by-challenges-like-us-blacklist.html>.

¹⁰Letter from Christopher Krebs, Former Director, CISA, to Jerry Nadler, Former Chairman, House Judiciary Committee (June 23, 2020), available at https://www.scribd.com/document/466960345/DHS-warns-about-China-made-DJI-drones?irclid=1s4WxhQbmxyNR9L2odz-41r2UkASfeUSXC5Ug0&irpid=10078&utm_source=impact&utm_medium=cpc&utm_campaign=affiliate_pdm_acquisition_Skimbit20%Ltd.&sharedid=nypost.com&irgwc=1.

¹¹Brian Harrell and Travis Moran, *The pressing threat of Chinese-made drones flying above U.S. critical infrastructure*, Cyberscoop (March 23, 2023) <https://cyberscoop.com/chinese-drone-threat-dji-regulation-critical-infrastructure/>.

¹²David Shortell, *DHS warns of 'strong concerns' that Chinese-made drones are stealing data* (May 20, 2019) <https://www.cnn.com/2019/05/20/politics/dhs-chinese-drone-warning/index.html>.

¹³PRC National Intelligence Law (as amended in 2018), China Law Translate, <https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/> (last visited May 31, 2023).

DJI Technology Co., as well as U.S. and other foreign organizations and citizens doing business or otherwise operating in the PRC would be required to share all information in their possession with the CCP.¹⁴ It is imperative that DHS be prohibited from purchasing and operating foreign-made UAS, particularly Chinese-made UAS, given the technology's significant capacity to collect sensitive information as well as the legal requirement for UAS crafted in the PRC to share such information with the CCP.

The Committee's intent is to safeguard sensitive information that may be collected by UAS deployed by DHS for the purpose of completing its various mission sets. Furthermore, the Committee's intent is to mitigate covered foreign countries, especially the PRC, from leveraging UAS to commit espionage or create risks to U.S. homeland security. It is also the Committee's intent to ensure that foreign adversarial countries are unable to compromise the work of the United States government through foreign-made UAS as well as domestic-made UAS that is implicated under the PRC's National Intelligence Law, as amended in 2018.

In the 117th Congress, on September 29, 2021, this unamended version of this bill passed the House of Representatives on suspension by voice vote. In the 118th Congress, this legislation was reintroduced. H.R. 1501 has bipartisan support and was reported favorably out of the Committee on Homeland Security by voice vote.

HEARINGS

The Committee held the following hearing in the 118th Congress that informed H.R. 1501:

On March 9, 2023, the Subcommittee on Counterterrorism, Law Enforcement, and Intelligence held a hearing entitled "Confronting Threats Posed by the Chinese Communist Party to the U.S. Homeland." The Subcommittee received testimony from the Honorable William R. Evanina, former Director of the National Counterintelligence and Security Center, Office of the Director of National Intelligence, Lieutenant General Joseph Guastella Jr., (Ret.), Senior Fellow, Mitchell Institute, the Honorable Kari A. Bingen, former Principal Deputy Under Secretary of Defense for Intelligence, Department of Defense, and Dr. Tyler Jost, Assistant Professor of Political Science and International and Public Affairs, Brown University.

On May 23, 2023, the Subcommittee on Counterterrorism, Law Enforcement, and Intelligence held a hearing entitled "A Security Sprint: Assessing the U.S. Homeland's Vulnerabilities to Chinese Communist Party Aggression." The Subcommittee received testimony from Jill M. Murphy, Deputy Assistant Director of Counterintelligence, Federal Bureau of Investigation, Iranga Kahangama, Assistant Secretary for Cyber, Infrastructure, Risk, and Resilience, Department of Homeland Security, and Tyrone Durham, Acting Director of the Nation State Threats Center, Office of Intelligence and Analysis, Department of Homeland Security.

¹⁴Murray Scot Tanner, *Beijing's New National Intelligence Law: From Defense to Offense*, Lawfare (July 20, 2017) <https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense>.

COMMITTEE CONSIDERATION

The Committee met on May 17, 2023, a quorum being present, to consider H.R. 1501 and ordered the measure to be favorably reported to the House, as amended, by a voice vote.¹⁵

COMMITTEE VOTES

Clause 3(b) of rule XIII requires the Committee to list the recorded votes on the motion to report legislation and amendments thereto.

No recorded votes were requested during consideration of H.R. 1501.

COMMITTEE OVERSIGHT FINDINGS

In compliance with clause 3(c)(1) of rule XIII, the Committee advises that the findings and recommendations of the Committee, based on oversight activities under clause 2(b)(1) of rule X, are incorporated in the descriptive portions of this report.

CONGRESSIONAL BUDGET OFFICE ESTIMATE, NEW BUDGET AUTHORITY, ENTITLEMENT AUTHORITY, AND TAX EXPENDITURES

With respect to the requirements of clause 3(c) of rule XIII and section 308(a) of the Congressional Budget Act of 1974, and with respect to the requirements of clause 3(c)(3) of rule XIII and section 402 of the Congressional Budget Act of 1974, the Committee adopts as its own the estimate of any new budget authority, spending authority, credit authority, or an increase or decrease in revenues or tax expenditures contained in the cost estimate prepared by the Director of the Congressional Budget Office.

H.R. 1501, UAS Act			
As ordered reported by the House Committee on Homeland Security on May 17, 2023			
By Fiscal Year, Millions of Dollars	2023	2023-2028	2023-2033
Direct Spending (Outlays)	0	0	0
Revenues	0	0	0
Increase or Decrease (-) in the Deficit	0	0	0
Spending Subject to Appropriation (Outlays)	0	+	not estimated
Increases <i>net direct spending</i> in any of the four consecutive 10-year periods beginning in 2034?	No	Statutory pay-as-you-go procedures apply?	No
		Mandate Effects	
Increases <i>on-budget deficits</i> in any of the four consecutive 10-year periods beginning in 2034?	No	Contains intergovernmental mandate?	No
		Contains private-sector mandate?	No
* = between zero and \$500,000.			

H.R. 1501 would prevent the Department of Homeland Security (DHS) from operating or procuring an unmanned aircraft system

¹⁵ H.R.1501—UAS Act, Congress.gov, <https://www.congress.gov/bill/118th-congress/house-bill/1501/all-actions> (last visited May 31, 2023).

(UAS) that is manufactured in or by a business entity headquartered in a foreign country that poses a threat to national security. The prohibition would also apply to software systems associated with UAS that store data or use a network located in such a country. The bill would allow DHS to waive the prohibition on a case-by-case basis upon notification to the Congress. H.R. 1501 also would require DHS to report to the Congress on the number of UAS subject to the prohibition currently operated by DHS and the threats they pose to national security.

DHS's current operations and policy are largely consistent with the bill's requirements and CBO estimates that any changes required under the bill would not require substantial action by the department. On that basis and the cost of similar reporting requirements, CBO estimates that implementing H.R. 1501 would cost less than \$500,000 over the 2024-2028 period. Any spending would be subject to the availability of appropriated funds.

The CBO staff contact for this estimate is Jeremy Crimm. The estimate was reviewed by H. Samuel Papenfuss, Deputy Director of Budget Analysis.

PHILLIP L. SWAGEL,
Director, Congressional Budget Office.

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 of 1995.

DUPLICATIVE FEDERAL PROGRAMS

Pursuant to clause 3(c) of rule XIII, the Committee finds that H.R. 1501 does not contain any provision that establishes or reauthorizes a program known to be duplicative of another Federal program.

STATEMENT OF GENERAL PERFORMANCE GOALS AND OBJECTIVES

Pursuant to clause 3(c)(4) of rule XIII, the objective of H.R. 1501 is to prohibit the Secretary of Homeland Security from operating or procuring certain foreign-made unmanned aircraft systems, and for other purposes.

CONGRESSIONAL EARMARKS, LIMITED TAX BENEFITS, AND LIMITED TARIFF BENEFITS

In compliance with rule XXI, this bill, as reported, contains no congressional earmarks, limited tax benefits, or limited tariff benefits as defined in clause 9(d), 9(e), or 9(f) of rule XXI.

ADVISORY COMMITTEE STATEMENT

No advisory committees within the meaning of section 5(b) of the Federal Advisory Committee Act (5 U.S.C. § 1004) were created by this legislation.

APPLICABILITY TO THE LEGISLATIVE BRANCH

The Committee finds that H.R. 1501 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 states that the Act may be cited as the “Unmanned Aerial Security Act” or the “UAS Act”.

Section 2. Prohibition on operation or procurement of certain foreign-made unmanned air craft systems

Subsection (a) paragraph (1) prohibits the Secretary of Homeland Security from operating, providing financial assistance for, or entering into or renewing a contract for the procurement of an unmanned aircraft system or drones that is manufactured in a covered foreign country or by a business entity domiciled in such foreign country; uses flight controllers, radios, data transmission devices, cameras, or gimbals manufactured in a covered foreign country; or by a business entity domiciled in a covered foreign country; uses ground control system or operating software developed in a covered foreign country or by a business entity domiciled in a covered foreign country; or uses network connectivity or data storage located in a covered foreign country or administered by a business entity domiciled in a covered foreign country.

Subsection (a) paragraph (2) prohibits the Secretary of Homeland Security from operating, providing financial assistance for, entering into, or renewing a contract for the procurement of a software operating system associated with a UAS that uses network connectivity or data storage located in a covered foreign country or administered by a business entity domiciled in a covered foreign country.

Subsection (a) paragraph (3) prohibits the Secretary of Homeland Security from operating, providing financial assistance for, entering into, or renewing a contract for the procurement of a system for the detection or identification of a UAS, which system is manufactured in a covered foreign country or by a business entity domiciled in a covered foreign country.

Subsection (b) authorizes the Secretary of Homeland Security to waive the prohibition under subsection (a) if the Secretary certifies in writing to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate that a UAS, a software operating system associated with a UAS, or a system for the detection or identification of a UAS described in any of paragraphs (1) through (3) of subsection (a) is required in the national interest of the United States; required for counter-UAS surrogate research, testing, development, evaluation, or training; or required for intelligence, electronic warfare, or information warfare operations, testing, analysis, and or training. The waiver must be submitted to the Committees specified no later than the date that is 14 days after the date on which a waiver is issued.

Subsection (c) details that the Act shall take effect 120 days after the date of enactment. Subsection (c) also details that no later than

60 days after the date of enactment of this Act, the Secretary shall establish a process by which the head of an office or component of DHS may request a waiver under subsection (b).

Subsection (d) directs the Secretary of Homeland Security to submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Government Affairs of the United States Senate a terrorism threat assessment and report on information relating to DHS's analysis of the threats posed by UAS operating in the United States, the number of UAS and related technologies in operation by DHS, including identifying the specific component or office of DHS, and information on how UAS and related technologies could be used to harm the national or economic security of the United States.

Subsection (e) defines the terms of a covered foreign country, the intelligence community, and an unmanned aircraft system. The term covered foreign country means a country that the intelligence community has identified as a foreign adversary in its annual Threat Assessment or the Secretary of Homeland Security in coordination with the Director of National Intelligence has identified as a foreign adversary. The terms intelligence community and an unmanned aircraft system have the same meaning of title 50 section 3003(4) and title 49 section 44801, respectively. Additionally, the term business entity in this bill has the meaning given in 15 U.S.C. 6764.