BILLING CODE: 3510-33

DEPARTMENT OF COMMERCE

Bureau of Industry and Security

15 CFR Part 791

[Docket No. 241213-0327]

RIN 0694-AJ72

Securing the Information and Communications Technology and Services Supply Chain: Unmanned Aircraft Systems

AGENCY: Bureau of Industry and Security, U.S. Department of Commerce.

ACTION: Advance notice of proposed rulemaking.

SUMMARY: In this advance notice of proposed rulemaking (ANPRM), the Department of Commerce's Bureau of Industry and Security (BIS) seeks public comment on issues related to transactions involving information and communications technology and services (ICTS) that are designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries, pursuant to Executive Order (E.O.) 13873, "Securing the Information and Communications Technology and Services Supply Chain," and that are integral to unmanned aircraft systems (UAS). This ANPRM will assist BIS in determining the technologies and market participants that may be appropriate for regulation in order to address undue or unacceptable risks to U.S. national security, including U.S. ICTS supply chains and critical infrastructure, or/and to the security and safety of U.S. persons.

DATES: Comments must be received on or before [INSERT DATE 60 DAYS AFTER PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: All comments must be submitted by one of the following methods:

• *The Federal eRulemaking Portal*: *https://www.regulations.gov* at docket number BIS-2024-0058.

• *Email directly to:* UnmannedAircraftSystems@bis.doc.gov. Include "RIN 0694-AJ72" in the subject line.

• *Instructions:* Comments sent by any other method, to any other address or individual, or received after the end of the comment period, may not be considered. For those seeking to submit business confidential information (BCI), please clearly mark such submissions as BCI and submit by email, as instructed above. Each BCI submission must also contain a summary of the BCI, clearly marked as public, in sufficient detail to permit a reasonable understanding of the substance of the information for public consumption. Such summary information will be posted on *regulations.gov.* Comments that contain profanity, vulgarity, threats, or other inappropriate language or content will not be considered.

FOR FURTHER INFORMATION CONTACT: Marc Coldiron, U.S. Department of Commerce, telephone: 202-482-3678. For media inquiries: Katherine Schneider, Office of Congressional and Public Affairs, Bureau of Industry and Security, U.S. Department of Commerce: OCPA@bis.doc.gov.

SUPPLEMENTARY INFORMATION:

I. Background

In E.O. 13873, "Securing the Information and Communications Technology and Services Supply Chain," (84 FR 22689 (May 17, 2019)) the President delegated to the Secretary of Commerce (Secretary) the authority granted under the International Emergency Economic Powers Act (IEEPA) (50 U.S.C. 1701, *et seq.*), to the extent necessary, "to deal with any unusual and extraordinary" foreign threat to the national security, foreign policy, or economy of the United States in connection with the national emergency declared by the President with respect to such threat (50 U.S.C. 1701(a)). In E.O. 13873, the President declared a national emergency with respect to the "unusual and extraordinary" foreign threat posed to the ICTS supply chain and has, in accordance with the National Emergencies Act (NEA), extended the declaration of this national emergency each year since E.O. 13873's publication (see 85 FR 29321 (May 14,

2020); 86 FR 26339 (May 13, 2021); 87 FR 29645 (May 13, 2022); 88 FR 30635 (May 11, 2023); and 89 FR 40353 (May 9, 2024)).

Specifically, the President identified the "unrestricted acquisition or use in the United States of [ICTS] designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries" as "an unusual and extraordinary" threat to the national security, foreign policy, and economy of the United States that "exists both in the case of individual acquisitions or uses of such technology or services, and when acquisitions or uses of such technologies are considered as a class" (E.O. 13873; see also 50 U.S.C. 1701(a)-(b)).

Once the President declares a national emergency, IEEPA empowers the President to, among other acts, investigate, regulate, prevent, or prohibit any "acquisition, holding, withholding, use, transfer, withdrawal, transportation, importation or exportation of, or dealing in, or exercising any right, power, or privilege with respect to, or transactions involving, any property in which any foreign country or a national thereof has any interest by any person, or with respect to any property, subject to the jurisdiction of the United States" (50 U.S.C. 1702(a)(1)(B)).

To address identified risks to U.S. national security from ICTS transactions, the President in E.O. 13873 imposed a prohibition on transactions determined by the Secretary, in consultation with relevant agency heads, to involve foreign adversary ICTS and to pose certain risks to U.S. national security, including U.S. ICTS supply chains and critical infrastructure, and to the security and safety of U.S. persons. Specifically, to fall within the scope of the prohibition, the Secretary must determine that the ICTS transaction: (1) involves ICTS designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, defined in E.O. 13873 section 3(b) as "any foreign government or foreign non-government person 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"; and (2):

A. "poses an undue risk of sabotage to or subversion of the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of information and communications technology or services in the United States;"

B. "poses an undue risk of catastrophic effects on the security or resiliency of United States critical infrastructure or the digital economy of the United States;" or

C. "otherwise poses an unacceptable risk to the national security of the United States or the security and safety of United States persons" (E.O. 13873 1(a)).

These factors are collectively referred to as "undue or unacceptable risks." Further, E.O. 13873 grants the Secretary the authority to design or negotiate mitigation measures that would allow an otherwise prohibited transaction to proceed (E.O. 13873 1(b)). The President also delegated to the Secretary the ability to promulgate regulations that, among other things, establish when transactions involving particular technologies may be categorically prohibited (E.O. 13873 2(a)-(b); see also 3 U.S.C. 301-302). Specifically, the Secretary may issue rules establishing criteria, consistent with section 1 of E.O. 13873, by which particular technologies or market participants may be categorically included in or categorically excluded from prohibitions established pursuant to E.O. 13873 (see E.O. 13873 2(b)). Any regulated transactions under E.O. 13873 must have a sufficient nexus to a foreign adversary, which, according to E.O. 13873's implementing regulations at 15 CFR 791.4, currently includes, China, People's Republic of (China), including the Hong Kong Special Administrative Region; Republic of Cuba (Cuba); Islamic Republic of Iran (Iran); Democratic People's Republic of Korea (North Korea); Russian Federation (Russia); and Venezuelan politician Nicolás Maduro (Maduro Regime).

II. Introduction

Pursuant to the authority delegated to the Secretary under E.O. 13873, BIS is considering proposing a rule to address the undue or unacceptable risks posed by certain transactions

involving ICTS integral to unmanned aircraft system (UAS) when the ICTS are designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries (foreign adversary ICTS). BIS is also considering whether there are mitigation measures that, if adopted, would allow UAS market participants to engage in transactions that would otherwise pose undue or unacceptable risks. The purpose of this ANPRM is to gather information to support BIS's potential development of a rule regarding foreign adversary ICTS integral to UAS. For the purposes of this rulemaking, unless terms are otherwise defined herein, this ANPRM will apply the definitions listed in 15 CFR 791.2.

III. Request for Comments

BIS is concerned that the involvement of foreign adversaries, notably China and Russia, in the design, development, manufacture, or supply of ICTS integral to UAS poses undue or unacceptable risk to U.S. national security, including U.S. ICTS supply chains and critical infrastructure, and to the security and safety of U.S. persons. As described in more detail below, these countries can leverage their political and legal frameworks to co-opt private entities for national interests, and those private entities maintain dominant market positions in the global commercial UAS sector. This dominance, particularly by China, provides ample exploitation opportunities. Further, both countries have shown a willingness to compromise U.S. infrastructure and security through cyber espionage. The potential for these countries to direct the actions of private entities for the purpose of exploiting ICTS supply chains heightens concerns about their participation in the U.S. UAS supply chain.

BIS seeks public input on several topics, including, but not limited to, certain definitions and BIS's assessment of how a class of transactions involving foreign adversary ICTS integral to UAS could present undue or unacceptable risks to U.S. national security and to the security and safety of U.S. persons. These risks relate to threats from foreign adversary-linked entities, the capabilities of UAS that may increase the likelihood of vulnerabilities, and the consequences to U.S. national security, including U.S. ICTS supply chains and critical infrastructure, and to the

security and safety of U.S. persons if these vulnerabilities are exploited or intentionally inserted by foreign adversary linked entities. BIS recognizes the benefits of UAS technologies and does not imply through this ANPRM that any particular UAS components, such as data transmission or connectivity devices, should not be used. These technologies benefit the United States by increasing efficiency in various critical infrastructure sectors such as agriculture, construction, transportation, and energy, leading to economic growth and improved public safety. However, in E.O. 13873, the President focused on addressing risks that ICTS transactions involving foreign adversaries might present to U.S. national security and to the security and safety of U.S. persons. Therefore, this ANPRM, which is being issued pursuant to the authorities granted to the Secretary under E.O. 13873, seeks public comment on potential ways to address undue or unacceptable risks to U.S. national security, including U.S. ICTS supply chains and critical infrastructure, -and to the security and safety of U.S. persons that may arise from foreign adversary ICTS integral to UAS. As part of BIS's efforts to understand UAS and their critical ICTS components, BIS solicits comments on the -ICTS most integral to UAS's data collection and connectivity capabilities and that are most vulnerable to compromise by an adversarial actor. Such ICTS might be included in any mitigation measures or prohibitions imposed in a potential rule, and could include, but is not limited to: (1) onboard computers responsible for processing data and controlling UAV flight; (2) communications systems including, but not limited to, flight controllers, transceiver/receiver equipment, proximity links such as Global Navigation Satellite Systems (GNSS) sensors, and flight termination equipment; (3) flight control systems responsible for takeoff, landing, and navigation, including, but not limited to, exteroceptive and proprioceptive sensors; (4) ground control stations (GCS) or systems including, but not limited to, handheld flight controllers; (5) operating software including, but not limited to, network management software; (6) mission planning software; (7) intelligent battery power systems; (8) local and external data storage devices and services; and (9) artificial intelligence (AI) software or applications. BIS also solicits input on mechanisms to mitigate the risks posed by foreign

adversary ICTS integral to UAS, such as potential design requirements, machine learning controls, implementation standards and protocols, cybersecurity firmware and/or software inputs, manufacturing integrity (*i.e.*, the security of the manufacturing process to ensure no foreign adversary manipulation) protection systems and procedures, or prohibitions.

Additionally, BIS seeks comment on whether it would be beneficial to create a process for the public to request specific authorization to engage in certain transactions involving foreign adversary ICTS integral to UAS by demonstrating that the parties to a particular transaction have implemented measures to adequately mitigate the risk to U.S. national security or to the security and safety of U.S. persons. BIS encourages public feedback to help inform the rulemaking process, particularly regarding the impact on U.S. ICTS supply chains and critical infrastructure of any prohibition or mitigation measures applicable to foreign adversary ICTS integral to UAS. BIS additionally encourages the submission of any public comments germane to the issues as described in this ANPRM.

a. Definitions

BIS requests comments on a definition of "unmanned aircraft systems" or UAS to use in a potential rule. BIS could define UAS as the International Trade Administration (ITA) does to mean "air vehicles and associated equipment that do not carry a human operator, but instead are remotely piloted or fly autonomously" (International Trade Administration, *Unmanned Aircraft Systems Overview* (accessed October 15, 2024), *https://www.trade.gov/unmanned-aircraft-systems/*). UAS, more colloquially known as "drones," is a generic term that can include, but is not exclusive to, remotely piloted aircraft systems or unmanned aerial vehicles. ITA's definition also states "[a] UAS generally consists of (1) an aircraft with no pilot on board, (2) a remote pilot station, (3) a [command-and-control] link, and (4) a payload specific to the intended application [or] operation, which often includes specialized cameras or other sensors that collect data for near term analysis" (International Trade Administration, *Unmanned Aircraft Systems Overview* (accessed October 15, 2024), *https://www.trade.gov/unmanned-aircraft-systems/*).

BIS is also contemplating the use of other definitions of UAS from the U.S. government, including the definition used by the Federal Aviation Administration (FAA), which defines UAS as "an unmanned aircraft and associated elements (including communication links and the components that control the unmanned aircraft) that are required for the operator to operate safely and efficiently in the national airspace system" (49 U.S.C. 44801(12)). The FAA defines an "unmanned aircraft" to mean "an aircraft that is operated without the possibility of direct human intervention from within or on the aircraft" (49 U.S.C. 44801(11)).

BIS also considered the definition of unmanned aerial vehicle (UAV) as used within BIS's Export Administration Regulations (EAR), which defines UAV as "[a]ny 'aircraft' capable of initiating flight and sustaining controlled flight and navigation without any human presence on board" (15 CFR 772.1). The EAR defines "aircraft" as "[a] fixed wing, swivel wing, rotary wing (helicopter), tilt rotor or tilt-wing airborne vehicle" (15 CFR 772.1). BIS considered the use of UAV versus UAS and believes UAV is too narrowly focused for future rulemaking purposes, as it only refers to the air vehicle itself and excludes other system elements, such as the ground control stations, communication links, and other associated components necessary for operation.

BIS is inclined to determine that ITA's definition may be more appropriate for purposes of potential regulation because, unlike the FAA and EAR definitions, it identifies specific components and systems that are integral to UAS. Such a definition may include UAS and UAS subsystems, such as control stations; data communications and navigation links or, more precisely, command and control and Non-Payload Communications (CNPC) links; payloads; flight termination systems; electronic launch and recovery equipment; recording capabilities for receiving live imagery; software or AI software and applications necessary for the operation of airborne systems; and the capability of remote software or firmware updates. Additionally, ITA's definition would incorporate some UAS known as actively tethered UAS, which use a load-rated tether that is physically attached to a ground station to provide continuous power and which may transmit data to and from the UAS, which allows the UAS to remain in the air for an extended

period of time. Please note that any definition determined by BIS to be appropriate for BIS rulemaking regarding UAS would not supersede any other legal definition of UAS used in other contexts.

Given the various definitions that could be utilized, this ANPRM seeks comment on the definitions to use in a potential rule regarding transactions involving ICTS integral to UAS, and specifically, but not limited to:

1. In what ways, if any, should BIS elaborate on or amend the potential definition(s) of UAS as stated above? If amended, how will the revised definition enable BIS to better address national security risks arising from classes of transactions involving ICTS integral to UAS?
2. Is the term UAS broad enough to include the aircraft systems that may combine flight controllers, global navigation satellite systems (GNSS) modules, cameras, communication devices, surveillance modules, navigation devices, sensors with control systems, and/or software with onboard and offboard data storage capabilities? Does a better term exist to include such aircraft systems within the definition's scope?
3. Are there other commonly used definitions for UAS that BIS should consider when defining a class of transactions involving ICTS integral to UAS, including definitions from industry, civil society, or international standards organizations? If so, why might those definitions be more appropriate for the purposes of a rule?
4. What is the appropriate focus of any BIS regulations in this sector, including, but not limited to, UAS platforms and subcomponent technology, UAS capabilities, or UAS end-user sectors, including entities providing services performed by UAS?
5. Are there commonly used definitions and standard capabilities for each of the following ICTS components, which BIS has preliminarily identified as integral to the UAS platform: (1) onboard computers responsible for processing data and controlling UAV flight; (2) communications systems including, but not limited to, flight controllers, transceiver/receiver equipment, proximity links such as GNSS sensors, and flight termination equipment; (3) flight control

systems responsible for takeoff, landing, and navigation, including, but not limited to, exteroceptive and proprioceptive sensors; (4) GCS or systems including, but not limited to, handheld flight controllers; (5) operating software including, but not limited to, network management software; (6) mission planning software; (7) intelligent battery power systems; (8) local and external data storage devices and services; (9) AI software or applications? Are there additional components that BIS should identify as integral to the UAS platform and, if so, are there commonly used definitions and standard capabilities for each component, such as the American Security Drones Act?

b. Risks associated with UAS

BIS is soliciting comment on the risks associated with foreign adversary ICTS integral to UAS, the rapidly advancing technological functionalities of UAS, and the increasing integration of UAS with U.S. critical infrastructure. Exponential advancements in UAS functionality have allowed for the rapid expansion of the UAS industry in recent years. Remote and autonomous control systems have been developed to support operational, safety, and environmental applications, minimizing physical strain and risks to operators in various fields. Advancements in this sector have reduced production and end user costs and increased the accessibility of UAS technology. In addition, UAS have become integral to various sectors of the economy, including: (1) agriculture, where they are used for crop monitoring and precision spraying; (2) the chemical industry, where they assist in pipeline inspections and hazardous material handling; (3) physical infrastructure and transportation, where they are employed for surveying, bridge inspections, and construction site management; (4) emergency response; (5) health care administration; (6) energy; and (7) media and entertainment.

Over the last decade, UAS have evolved to more sophisticated models with improved functionalities, including enhanced connected technologies such as advanced flight controllers, multi-GNSS and GNSS modules, cameras, receivers, and AI software and applications, which have enabled greater autonomy, precision in navigation, enhanced surveillance capabilities, and

seamless integration with various applications across industry. These new technologies require signal and communication software to collect vast amounts of data, and in turn may increase attack vectors for malicious actors to exploit.

Commercial UAS have been increasingly adopted in critical infrastructure sectors, as defined in National Security Memorandum-22 of April 2024 (see Grand View Research, *Drone Market Size, Share & Trends Analysis Report by Component (Hardware, Software, Services), By Product, By Technology, By Payload Capacity, By Power Source, By End-use, By Region, and Segment Forecasts, 2024 – 2030* (accessed October 15, 2024), *https://www.grandviewresearch.com/industry-analysis/drone-market-report*; see also The White House, *National Security Memorandum on Critical Infrastructure Security and Resilience* (April 30, 2024), *https://www.whitehouse.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/*). UAS used in these sectors often rely on the same aircraft used by recreational drone enthusiasts, but in many cases the UAS used to support critical infrastructure have longer flight times, can lift heavier and more complex payloads, can fly beyond visual line of sight, and have the durability to fly through rough weather conditions. UAS capable of lifting and carrying payloads for extended periods of time pose a specific and aggravated risk of both data collection and manipulation, as well as remote access that could be misused for destructive purposes. As critical infrastructure becomes more reliant on commercial UAS, their remote incapacitation by a foreign adversary creates increased risk to U.S. national security and to the security and safety of U.S. persons.

Malign remote access to UAS could be used to harm or damage physical infrastructure via intentional collisions, the delivery of kinetic payload, or could result in altered sensitive readings on critical infrastructure data. These risks can be exacerbated if the ICTS integral to UAS is designed, developed, manufactured, or supplied, by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary. Accordingly, BIS requests public comment on the undue or unacceptable risks posed by transactions involving foreign adversary

ICTS integral to UAS technology. BIS seeks comments on the following topics but encourages the submission of any comments germane to the issues discussed in this ANPRM:

6. BIS identified data exfiltration and remote access control as the two primary areas of risk associated with transactions involving foreign adversary ICTS integral to UAS technology. Are there other risks or factors contributing to the risk that BIS has not considered in the above analysis?

7. Which specific sectors or elements of critical infrastructure operated by private organizations, specifically within the commercial market, are most at risk if UAS technology is compromised?

c. Threat Posed by Foreign Adversaries

Foreign adversaries like China and Russia have established certain legal and regulatory frameworks through which they could compel entities under their jurisdiction to comply with requests for information regarding U.S. persons or access to systems in the U.S. ICTS supply chain. China has implemented a series of laws (*e.g.*, the National Intelligence Law of 2017, the Cybersecurity Law of 2017, the Personal Information Protection Law (PIPL) of 2021, the National Security Law of 2015) that mandate cooperation with China's cybersecurity efforts, intelligence operations, and the protection of national security interests by individuals and entities subject to the jurisdiction of China. These laws require network operators and technology companies to assist public security agencies in safeguarding cybersecurity and providing access to data stored within China's borders (see Department of Homeland Security, *Data Security Business Advisory* (July 11, 2022), *https://www.dhs.gov/sites/default/files/publications/20_1222_data-security-business-advisory.pdf*). Specifically, the National Security Law of 2015 imposes obligations that require organizations and individuals to cooperate with Chinese authorities on undefined 'matters of national security,' potentially requiring technology companies to expose the personal information of U.S. citizens or companies (see CNA, *China's National Security Laws:*

Implications Beyond Borders (December 2023), *https://www.cna.org/quick-looks/2023/China-national-security-laws-implications-beyond-borders.pdf*).

Similarly, Russian legislation (*e.g.*, Federal Law No. 40-FZ, "On the Federal Security Service"; Federal Law No. 144-FZ, "Open-Investigative Activity"; Federal Law No. 97-FZ, "On Amendments to the Law") grants the Russian government direct access to Russian corporations' activities and facilities. Using this authority, the Russian government could access companies' data and consumer information and mandate that companies cooperate with the Federal Security Services (FSB) to assist with counterintelligence actions, which can include installing government equipment on companies' infrastructure for data collection. These laws compel Russia-based telecommunications providers, Internet service companies, and other entities to assist Russian security agencies in investigations and surveillance, ensuring compliance with national security imperatives (see Federal Law No. 374-FZ, "On Amending Federal Law 'On Combating Terrorism' And Certain Legislative Acts of the Russian Federation Regarding the Establishment of Additional Counter-Terrorism Measures and Public Security").

Within the United States, products developed by China-based entities make up at least 75 percent of the UAS consumer market (see Lukas Schroth, *Drone Market Shares in the USA After China-US Disputes*, Drone Industry Insights (March 2, 2021), *https://droneii.com/drone-market-shares-usa-after-china-usa-disputes*; see also David Kitron, *Game of Drones: Chinese Giant DJI Hit by U.S. Tensions, Staff Defections*, Reuters (March 8, 2021), *https://www.reuters.com/article/us-usa-china-tech-dji-insight/game-of-drones-chinese-giant-dji-hit-by-u-s-tensions-staff-defections-idUSKBN2AZ0PV/*). The large market share of China-based entities allows China to exercise control over the supply chain and deny access to UAS technology. With the added element of China's ability to exercise jurisdiction over the primary producers of UAS products and components globally, China is unmatched in its control over crucial UAS elements used for commercial needs. The preeminence of China-based entities in the U.S. market provides China, through its established legal framework and control over

persons subject to its jurisdiction, a significant opportunity to collect U.S. persons' data and potentially deny services to the United States and its allies in response to unfavorable policies or conflicts.

Russia, in comparison to China, comprises a relatively small portion of the global UAS market share, but has announced its intention to heavily invest in developing Russia's UAS domestic market over the next few years to be less reliant on external manufacturers (see, *e.g.*, *Russia plans to produce 18,000 drones annually by late 2026 — first deputy premier*, TASS (April 27, 2023), *https://tass.com/economy/1610899*). As of 2023, Russia reportedly produced only 6,000 UAS and aims to boost domestic drone production for various industry sectors (see Martin Forusek, *Russian official: Russia aims to produce over 32,000 civilian drones annually by 2030,* Kyiv Independent (January 6, 2024), *https://kyivindependent.com/russian-official-russia-aims-to-produce-32-000-drones-annually-by-2030/).* While the nascent state of Russia's UAS market may not currently pose risks to U.S. national security, including U.S. ICTS supply chains and critical infrastructure, and to the security and safety of U.S. persons in the commercial space, the projected growth of Russia's domestic market suggests national security risks will emerge if left unchecked. The strategic investments being made in Russia mirror the same efforts made by China in its own markets and may position Russia as a high-volume supplier in the UAS space in the near future.

Despite their different current UAS market shares, China and Russia have demonstrated that they are capable of engaging in cyber activities that seek to harm U.S. critical infrastructure and national security for strategic advantage. According to the Office of the Director of National Intelligence, China's cyber espionage pursuits and the export of surveillance, information, and communications technologies by China-based industries increase the threats of aggressive cyber operations against the United States and the suppression of the free flow of information in cyberspace (see Office of the Director of National Intelligence, *Annual Threat Assessment* (2024), *https://www.dni.gov/files/ODNI/documents/assessments /ATA-2024-Unclassified-*

Report.pdf). Additionally, Russia has long exploited vulnerabilities targeting critical infrastructure in the United States as well as in allied and partner countries (see Cybersecurity and Infrastructure Security Agency, *Hunting Russian Intelligence "Snake" Malware* (May 9, 2023), *https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-129a*). Whether through pre-positioning attacks or exploiting software vulnerabilities, China and Russia have exhibited their intent and capability to compromise U.S. national security, including U.S. ICTS supply chains and critical infrastructure, and the security and safety of U.S. persons.

Further, foreign adversaries, such as China or Russia, could direct UAS companies subject to their jurisdiction to engineer vulnerabilities into their products, exploit existing vulnerabilities, or push malicious updates, compromising these products without the UAS owner's knowledge. In the past, for example, China-based UAS companies have pushed firmware updates to implement no-fly restrictions that would disable their UAS in conflict zones defined by the company (see, *e.g.,* Haye Kesteloo*, Autel Robotics Implements No-Fly Zones in Conflict Areas to Prevent Drone Misuse,* DroneXL (December 24, 2023)*, https://dronexl.co/2023/12/24/autel-robotics-drone-no-fly-zones-conflict/*; Gareth Corfield, *Drone maker DJI quietly made large chunks of Iraq, Syria no-fly zones*, The Register (April 26, 2017), *https://www.theregister.com/2017/04/26/dji_drone_geofencing_iraq_syria/*). These UAS no-fly zones can also be altered through non-commercial methods by disabling UAS safety features (see, *e.g.*, Support, *No-Fly Zones (NFZ) Explained*, Drone-Hacks Wiki (last edited June 18, 2024), *https://wiki.drone-hacks.com/en/nfz-explained*). As of 2024, these alterations can be implemented across several China-based UAS models (see, *e.g.*, Drone-Hacks, *Available Hacks* (accessed October 15, 2024), *https://drone-hacks.com/available-hacks/* (an illustrative example of a website that allows users to download software to modify a drone's operating system to operate outside of specified no fly zones)). Pushing forced updates that disable UAS in predefined zones and circumventing safety features demonstrate two vectors through which a foreign adversary could abuse its access and influence over a company intentionally to target

UAS products owned by U.S. persons or operated in the United States, disrupt their operation, and in turn severely impact U.S. national security, including the U.S. ICTS supply chain and critical infrastructure, and the security and safety of U.S. persons.

This ANPRM seeks comments on the role of persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary in the U.S. supply chain for ICTS components integral to UAS. For clarity, this ANPRM uses the term "UAS companies" to refer to the manufacturers or distributors of a finished UAS product, like a drone, while the term "UAS Original Equipment Manufacturers" (OEMs) refers to the producers of the UAS components, including the tier 1, tier 2, and tier 3 suppliers. The term "UAS service providers" refers to entities responsible for desktop and mobile applications supporting UAS. A single company, depending on its products, could be a UAS company, OEM, and service provider all at once. BIS seeks comments on the below topics but encourages the submission of any comments germane to the issues discussed in this ANPRM:

8. In this section, BIS identified threats posed by transactions involving ICTS integral to UAS with a nexus to China or Russia. Has BIS fully captured and articulated the threat posed by transactions involving such ICTS? If not, what additional threats should BIS consider?

9. Do other foreign adversaries identified in 15 CFR 791.4, such as Iran, North Korea, Cuba, and the Maduro Regime of Venezuela, pose similar risks to the UAS ICTS supply chain that BIS should consider? Are there specific persons or entities with a nexus to these foreign adversaries that BIS should consider?

10. Which ICTS components integral to UAS are designed, developed, manufactured, or supplied predominantly or exclusively by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary?

a. Are UAS companies capable of tracking and reporting the sources of these ICTS components?

b. Are there specific ICTS components that UAS companies focus on when evaluating their supply chains for involvement with foreign adversary linked entities?

11. What are the potential tradeoffs of a rule prohibiting the resale or rental in the United States of UAS or UAS components that are designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary?

12. What are the software applications, whether freeware or requiring an account or purchase, that companies within the UAS supply chain generally develop or distribute in support of UAS, and/or sell or resell within the United States or to U.S. persons?

a. What is the provenance of all source code for such software applications? What do the distribution channels for such software applications look like (*e.g.*, direct, follow components, aftermarket)?

b. Please identify any significant third parties that develop source code for UAS OEM's software product lines.

13. Please describe the ICTS supply chain for UAS that are used or sold in the United States. Particularly useful responses may include information regarding:

a. Market leaders for each distinct phase of the supply chain for ICTS integral to UAS (*e.g.*, design, development, manufacturing, or supply) including, but not limited to: (1) UAS companies; (2) OEMs, including tier one, tier two, and tier three suppliers; and (3) service providers.

b. Geographic locations where software (*e.g.*, product operating systems or waypoint software), hardware (*e.g.*, light detection and ranging (LiDAR) sensors), or other ICTS integral to UAS in use in the United States, are designed, developed, manufactured, or supplied.

c. The length of time it typically takes to conduct due diligence on UAS vendors, how long the design phase is for UAS, and how quickly UAS companies can make changes to the supply chain.

14. Which ICTS components integral to UAS, including but not limited to those identified in this ANPRM, pose the greatest risk to U.S. national security, including U.S. ICTS supply chains and

critical infrastructure, or to the security and safety of U.S. persons if they are foreign adversary ICTS?

d. Capabilities of UAS that may increase the likelihood of vulnerabilities that foreign adversary linked entities could exploit.

Data Collection

UAS incorporate numerous ICTS components including sensors to gather environmental information, actuators to enable remote or autonomous movements, telecommunications equipment to receive signals necessary for flight, and software with intelligent algorithms to execute actions based on the gathered data. UAS for commercial or military purposes may incorporate additional equipment to collect more complex data, including multispectral sensors, thermal cameras, infrared sensors, and radar. These sensors may collect and transmit a wide variety of sensitive data (*e.g.*, critical infrastructure facility layouts which could be used to plot potential avenues for sabotage of such facilities). In general, data collected by UAS can be stored in multiple locations depending on the specifications of the UAS and user decisions, including on an internet-connected device such as a mobile phone or a computer, on a radio control device, on a hard drive or personal server, or on a cloud platform provided by UAS companies. In some instances, UAS companies state in their privacy policies that data may be stored in data centers located outside of the user's home country, to include where the UAS company is headquartered.

BIS seeks to better understand the data collection capabilities including intelligent machine learning algorithms of UAS and the ICTS components therein. In particular, BIS seeks further comment on the following topics but encourages the submission of any comments germane to the issues discussed in this ANPRM:

15. What are the general data collection capabilities of UAS? What is the level of aggregation and scale of data that UAS can collect on U.S persons, entities, geography, and infrastructure?

a. Who besides the operator of the UAS generally has authorized access to, or control of, data collected by UAS?

b. How is the data collected by UAS sold or integrated into data markets?

16. What are the UAS industry standard policies or procedures, if any, governing how data generated by, owned by, or otherwise associated with U.S. persons is stored, managed, processed, gathered, or protected in or on data-related services equipment located outside of the United States? BIS defines "data-related services equipment" as hardware used to receive, store, process or transmit data in support of data-related services, including routers, firewalls, gateways, switches, servers, load-balancers, intrusion detection systems, domain name systems, and storage area networks.

17. Are there standards or best practices for data retention and/or data disposition policies or procedures, involving data-related services equipment located outside the United States following the termination of any UAS account services by U.S. persons?

18. What are the standard policies or procedures related to UAS companies' and UAS OEMs' review of or access to data generated by, owned by, or otherwise associated with U.S. persons?

19. Are there industry standard policies or procedures establishing how UAS companies must or should protect the privacy of data generated by, owned by, or otherwise associated with U.S. persons?

20. What cybersecurity measures, authentication, or controls do UAS service providers and other companies supporting the UAS supply chain use to mitigate risks surrounding data collection, access, storage, processing, and exfiltration?

21. Is it standard for UAS companies to have data-related services equipment located outside of the United States that, at any time, UAS companies use to store, collect, process, analyze, share, distribute, or manage data generated by, owned by, or otherwise associated with U.S. persons?

22. How are UAS integrated in critical infrastructure sectors? Which of these integrated UAS services, if any, are particularly unique or of a sensitive nature such that a disruption to the UAS supply chain would create a gap for the sector?

23. Which sensors in or on UAS that are typically used in critical industries (*e.g.*, agricultural, chemical, construction, energy, telecommunication) are able to collect or transmit data or have connection capabilities?

a. Are there official aftermarket modification or customization options available for these types of sensors?

b. Are there any standard requirements for these sensors?

24. What is the standard practice for data sharing relationships between UAS companies and individuals or entities within the United States?

a. Are there agreements between UAS companies and cloud computing service providers that require the exclusive or prioritized use of that cloud service's network infrastructure? If so, please provide examples of how those agreements operate.

b. In industries in the United States where UAS are used to collect data, do companies share the data they collect with other companies? For what purpose (if not for the primary purpose of data collection)?

25. Are there any standard assessments, audits, or evaluations, internal or by an external party, of UAS companies' data privacy policies related to any data generated by, owned by, or otherwise associated with U.S. persons?

26. What role do specific remote sensing ICTS components serve for data collection by UAS? Particularly useful responses will describe the data collection role of the following components:

a. Imagery (RGB and Multi-spectral), 3-Dimensional, or Acoustic Sensors;

b. Particle Sensors (regardless of wavelength);

c. Radio Frequency Sensors;

d. Proximity and Navigation Sensors;

e. Electro-Magnetic Sensors; and/or

f. Other Sensors (including inertial).

27. How often are software applications related to the operation of UAS installed on a UAS user's phone? What policies govern the application's access to other information on the user's phone?

28. What systems, sensors, or equipment do UAS and their affiliated UAS operators use when not navigating or storing data over mobile networks?

29. How do UAS operators secure data that is transmitted, received, or stored during the normal operation of a UAS without connecting to the internet?

Remote Access and Control

Connectivity features in UAS have raised significant concerns regarding illicit remote access and security vulnerabilities (see, *e.g.*, Department of the Army, *Discontinue Use of Da Jiang Innovation (DJI) Corporation Unmanned Aircraft Systems* (August 2017), *https://www.suasnews.com/2017/08/us-army-calls-units-discontinue-use-dji-equipment/*). As UAS become increasingly sophisticated and equipped with advanced communication technologies such as Wi-Fi, Bluetooth, cellular connections, or other cellular communications technologies, the risk of unauthorized access to and control over UAS by malicious actors may grow. The integration of advanced communication technologies may allow malicious actors to intercept or hijack communication signals between a UAS and its controller, potentially leading to unauthorized access to sensitive data or control over the UAS itself.

Malicious actors could gain illicit access to cloud platforms used by UAS to store data or authorize remote control access and use that access to determine the location of a UAS and pilot (see Andy Greenberg, *This Hacker Tool Can Pinpoint a DJI Drone Operator's Exact Location*, Wired (March 2, 2023), *https://www.wired.com/story/dji-droneid-operator-location-hacker-tool/*). Once malicious actors gain such access, they can obfuscate their identities to obtain U.S. persons' sensitive information and data related to critical infrastructure. For example, researchers studying this issue have been successful in reverse engineering the radio frequency that controls a UAS and have been able to pinpoint the position of the UAS, the UAS home point, and the

remote pilot's location (see Nico Schiller, *et al., Drone Security and the Mystery Case of DJI's DroneID* (March 2023), *https://www.ndss-symposium.org/wp-content/uploads/2023/02/ndss2023_f217_paper.pdf*). Further, unauthorized UAS access may provide avenues for malicious actors to infiltrate drone operations within critical infrastructure companies, compromising their functionality and security. The potential consequences of compromised UAS systems are significant. Malicious actors' access to UAS could lead to the exfiltration of sensitive data, including real-time video feeds and geolocation information, which can be used to gather intelligence and conduct surveillance to threaten U.S. national security, including U.S. ICTS supply chains and critical infrastructure, or the security and safety of U.S. persons.

To understand the vulnerabilities inherent in UAS, BIS requests comments regarding specific ICTS components that enable UAS connectivity, such as network connectivity chips, operating software, AI software and machine learning applications, and data transmission devices. These components, which facilitate UAS communication with external networks, are susceptible to various forms of potential UAS cyber vulnerabilities if not properly secured. Supply chain security for these components may be essential. Compromised network connectivity chips, for example, may introduce backdoors or other malicious functionalities during the manufacturing process, which may be triggered when the UAS is activated. UAS could also be compromised through the corruption and injection of artificial intelligent code during the supply chain process in order to introduce vulnerabilities or functionalities affecting data access and UAS control, for example. The supply chain may be manipulated by foreign adversaries who seek to exploit vulnerabilities at various stages of production and distribution. Understanding and mitigating these risks by implementing comprehensive security assessments and standards may be vital for ensuring the integrity and security of UAS communication capabilities. Enhanced scrutiny of the UAS supply chain, especially regarding foreign adversary ICTS components, may be necessary to safeguard against potential threats from foreign

adversaries. As such, BIS seeks to understand the following topics in greater detail but welcomes any other comments germane to the issues discussed in this ANPRM:

30. What is the physical range of connectivity for UAS systems for commercial use?

31. Where is data stored on the physical UAS if any? Where is data that a UAS captures during routine operations stored off the physical UAS?

a. How long is data stored on and off the UAS platform?

32. What, if any, industry standard policies or procedures govern how UAS communicate, what kinds of information UAS can communicate, with what they can communicate, and which components enable, store, or analyze these communications?

33. What controls or procedures govern or should govern the use of AI in UAS?

34. What types of remote access or control do OEMs have over their UAS? Please also describe under what circumstances an OEM would require remote access or control.

35. To what extent can individual sensors and components communicate independently from the UAS Operating System (OS)?

36. What cybersecurity standards and best practices exist for the UAS supply chain? How do UAS OEMs supplement existing cybersecurity standards and best practices at each step of the UAS supply chain, including design, manufacturing, and maintenance?

37. How do UAS OEMs or UAS operators integrate payloads and related components from third parties into their software, OS, and AI software and applications?

38. Who are the third parties that commonly provide payloads and component parts (*e.g.*, sensors, payloads, cameras) for integration into UAS production?

a. Which, if any, of these third parties are owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary? Which, if any, of these third parties are owned by entities that operate under the laws of a foreign adversary? Where are these third parties incorporated and physically located? Please provide factual support where possible.

39. What ICTS components, other than payloads and related components, are made by non-U.S. third parties (*i.e.*, not the U.S. UAS OEM) for incorporation into UAS? Where are these component parts made? Where are the UAS assembled, and what entity (*e.g.*, OEM, third party servicer, or user/operator) would typically incorporate or integrate these additional components into a UAS?

40. Who provides and is responsible for cybersecurity updates to software, firmware, and AI software and applications for component parts integrated into UAS (*e.g.*, sensors, camera, payload)?

e. Consequences of Foreign Adversary Involvement in ICTS Integral to UAS

The ability of a foreign adversary to direct or control private companies through applicable legal frameworks, combined with the possible exploitation of vulnerabilities in the increasingly capable ICTS components integral to UAS, poses a significant threat of data exfiltration and malicious remote access. This could lead to severe, and in some instances catastrophic, consequences for U.S. national security, including U.S. ICTS supply chains and critical infrastructure, and for the security and safety of U.S. persons.

Through foreign adversary ICTS integral to UAS, the intelligence agencies of foreign adversaries could exfiltrate, collect, and aggregate a wide range of sensitive data on U.S. persons and critical infrastructure held by companies in the UAS ICTS supply chain. The data collected by UAS or by a connected device could include locations, for example, of military installations or critical infrastructure including water infrastructure or energy generation or storage facilities, flight paths, audio and video recordings, as well as information about operators' identities, finances, contacts, operator base locations, and operating sector, including critical infrastructure, which can be collected by UAS or by a connected device.

In addition, denial of service through backdoors embedded in a UAS's software could enable a foreign adversary linked entity under certain conditions to obtain control over various UAS functions, including the ability to disable the UAS completely. To illustrate using an

example noted generally above, in December 2023, a China-based UAS manufacturer rolled out a firmware update to their UAS that disabled any UAS located in "conflict zones" defined by the company to include Gaza, West Bank, Israel, Russia, Ukraine, and Taiwan, among others. Once the UAS entered one of the conflict zones with the downloaded update, it would cease functionality. Users would only be able to continue operation by refusing to download the update to the detriment of the long-term functionality of the UAS, as it would effectively bar the users from receiving future updates (see Haye Kesteloo, *Autel Robotics Implements No-Fly Zones in Conflict Areas to Prevent Drone Misuse*, DroneXL (December 24, 2023), *https://dronexl.co/2023/12/24/autel-robotics-drone-no-fly-zones-conflict/*). If abused by a malicious actor, pushed updates like this could open users up to the risk of newly defined and restricted "zones" that could affect the use and control of their UAS. A foreign adversary could exploit firmware updates of this type by exercising influence or control over a UAS service provider and instructing them to push a certain update.

BIS seeks to better understand how UAS OEMs may impact UAS functionality through their incorporated ICTS components. In particular, the ANPRM seeks further comment on the following topics but encourages the submission of any comments that are germane to the issues discussed in this ANPRM:

41. In what instances, and how, would OEMs be able to terminate functionality of a UAS (*i.e.*, denial of service)?

a. What are the standards and best practices governing the ability of OEMs to terminate functionality of a UAS?

b. Are there instances in which a third party or a subcomponent maker (*e.g.*, a maker of sensors) could remotely deny service to and fully or partially terminate functionality of a UAS or its respective sensor or component independently of the OEM?

c. Once service is denied or functionality is terminated, what are the standards and best practices for reinstating full operability?

d. Are there instances in which a UAS and its subcomponents can use any inherent connectivity they possess to connect to other devices, the cloud, or connected software applications online but be insulated against denial-of-service updates or patches by the OEM?

f. Mitigations and Authorizations

In addition to the topics discussed above, this ANPRM seeks comment on processes and mechanisms that BIS could implement in a potential rule to authorize otherwise prohibited ICTS transactions if the parties to such transactions adopt certain mitigation measures or otherwise mitigate the undue and unacceptable risks to U.S. national security, including U.S. ICTS supply chains and critical infrastructure, or to the safety and security of U.S. persons. In particular, the ANPRM seeks further comment on the following topics but encourages the submission of any comments that are germane to the issues discussed in this ANPRM:

42. Are there instances in which granting a temporary authorization to engage in otherwise prohibited UAS ICTS transactions would be necessary to avoid supply chain disruptions or other unintended consequences and in the interest of the United States?

43. Which, if any, categories or classifications of end users should BIS consider excluding from any prohibitions on transactions involving foreign adversary ICTS integral to UAS because transactions involving such end users would not pose an undue or unacceptable risk?

44. For what categories of ICTS transactions relating to UAS should BIS require a specific authorization before the transaction is permitted in the United States?

45. Please comment on potential requirements for authorizations and certifications for industry participants (*e.g.*, assemblers, manufacturers, dealers, sellers) filed electronically with BIS.

46. What certification or validation process should be implemented in order to validate mitigation actions taken? Should third-party testing and evaluation occur, and at what stage in the process should this testing and evaluation occur in order to validate mitigation actions?

g. Economic Impact

BIS is mindful that any regulation of transactions involving foreign adversary ICTS integral to UAS could have significant economic impacts on sectors that have incorporated this technology into their processes and may rely on UAS. For example, BIS recognizes regulations on these transactions could pose supply chain obstacles that could affect UAS and UAS component prices. BIS is concerned, however, about the short-term and long-term consequences of UAS and UAS supply chain abuse by foreign adversaries. Accordingly, this ANPRM seeks further comment on the following topics but encourages the submission of any comments that are germane to the issues discussed in this ANPRM:

47. What, if any, anticompetitive effects may result from regulation of transactions involving foreign adversary ICTS integral to UAS as contemplated by this ANPRM? And what, if anything, can be done to mitigate the anticompetitive effects?

48. What data privacy and protection impacts to U.S. businesses or the public, if any, might be associated with the regulation of transactions involving foreign adversary ICTS integral to UAS contemplated in this ANPRM? What are the benefits and costs, if any, of these impacts?

49. What additional economic impacts to U.S. businesses or the public, if any, might be associated with the regulation of transactions involving foreign adversary ICTS integral to UAS contemplated by this ANPRM?

a. If responding from outside the United States, what economic impacts to local businesses and the public, if any, might be associated with regulations of transactions involving foreign adversary ICTS integral to UAS in the United States?

50. What actions can BIS take, or provisions could it add to any proposed regulations, to minimize potential costs borne by U.S. businesses or the public?

a. If responding from outside the United States, what actions can BIS take, or what provisions could it add to any proposed regulations, to minimize potential costs borne by local businesses or the public?

Elizabeth L.D. Cannon,

Executive Director, Office of Information and Communications Technology and Services.

[FR Doc. 2024-30209 Filed: 1/2/2025 8:45 am; Publication Date: 1/3/2025]