PUBLIC NOTICE

Federal Communications Commission
45 L Street NE
Washington, DC 20554

News Media Information 202-418-0500
Internet: www.fcc.gov

DA 25-1086
Released: December 22, 2025

PUBLIC SAFETY AND HOMELAND SECURITY BUREAU ANNOUNCES ADDITION OF UNCREWED AIRCRAFT SYSTEMS (UAS) AND UAS CRITICAL COMPONENTS PRODUCED ABROAD, AND EQUIPMENT AND SERVICES LISTED IN SECTION 1709 OF THE FY2025 NDAA, TO FCC COVERED LIST

WC Docket No. 18-89, ET Docket No. 21-232, EA Docket No. 21-233

The Federal Communications Commission's (FCC or Commission) Public Safety and Homeland Security Bureau (PSHSB) maintains a list of equipment and services (Covered List) that have been determined to "pose an unacceptable risk to the national security of the United States or the security and safety of United States persons."[1] Pursuant to section 2 of the Secure and Trusted Communications Networks Act of 2019 (Secure Networks Act),[2] section 1709 of the Servicemember Quality of Life Improvement and National Defense Authorization Act for Fiscal Year 2025 (FY2025 NDAA),[3] and sections 1.50002(a) and 1.50003 of the Commission's rules,[4] PSHSB announces the addition of uncrewed aircraft systems (UAS) and UAS critical components produced in foreign countries to the Covered List. We also add communications and video surveillance equipment and services listed in FY2025 NDAA section 1709. We make these additions to the Covered List based on a National Security Determination made by an Executive Branch interagency body with appropriate national security expertise, including appropriate national security agencies.[5]

[1] Secure and Trusted Communications Networks Act of 2019, Pub. L. No. 116-124, 133 Stat. 158 (2020) (codified as amended at 47 U.S.C. §§ 1601-1609) (Secure Networks Act); 47 CFR §§ 1.50002, 1.50003. For the current version of the Covered List, *see* Federal Communications Commission, *List of Equipment and Services Covered By Section 2 of The Secure Networks Act*, https://www.fcc.gov/supplychain/coveredlist (last updated July 23, 2025).

[2] 47 U.S.C. § 1601.

[3] Servicemember Quality of Life Improvement and National Defense Authorization Act for Fiscal Year 2025, Pub. L. No. 118-159, § 1709, 138 Stat. 1773, 2209-10 (2024) (FY2025 NDAA). Section 1709 of the FY2025 NDAA directs the Commission to update the Covered List with respect to certain unmanned aircraft systems equipment and services when certain conditions are met. The statute directs the Commission to update the Covered List if there is a determination by "an appropriate national security agency" that certain communications or video surveillance equipment or services "pose unacceptable risk to the national security of the United States or the security and safety of United States persons."

[4] 47 CFR §§ 1.50002(a), 1.50003; *see also* Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs, WC Docket No. 18-89, Second Report and Order, 35 FCC Rcd 14284 (2020) (*Supply Chain Second Report and Order*).

[5] *See* 47 U.S.C. § 1601(c)(1); FY2025 NDAA §§ 1709(a)(1), (c)(1). The White House convened an Executive Branch interagency body with appropriate national security expertise, including appropriate national security agencies identified in the Secure Networks Act. *Id*. §§ 1601(c)(4), 1608(2). The National Security Determination is attached in full in Appendix B to this Public Notice.

National Security Determination. On December 21, 2025, we received a National Security Determination regarding the unacceptable risks posed by UAS and UAS critical components that are produced in foreign countries. Among other points, the National Security Determination states that:

"UAS and UAS critical components must be produced in the United States. This will reduce the risk of direct UAS attacks and disruptions, unauthorized surveillance, sensitive data exfiltration, and other UAS threats to the homeland. Furthermore, it will ensure our domestic UAS and UAS critical component manufacturing is resilient and independent, a critical national security imperative. UAS are inherently dual-use: they are both commercial platforms and potentially military or paramilitary sensors and weapons. UAS and UAS critical components, including data transmission devices, communications systems, flight controllers, ground control stations, controllers, navigation systems, batteries, smart batteries, and motors produced in a foreign country could enable persistent surveillance, data exfiltration, and destructive operations over U.S. territory, including over World Cup and Olympic venues and other mass gathering events. U.S. cybersecurity and critical infrastructure guidance has repeatedly highlighted how foreign manufactured UAS can be used to harvest sensitive data, used to enable remote unauthorized access, or disabled at will via software updates."[6]

Based on these findings, the Executive Branch interagency body, including several appropriate national security agencies, concluded that all the following equipment and services should be added to the FCC's Covered List because they pose an unacceptable risk to the national security of the United States and to the safety and security of U.S. persons: UAS produced in a foreign country pose an unacceptable risk to the national security of the United States and to the safety and security of U.S. persons and should be included on the FCC's Covered List, unless the Department of War or the Department of Homeland Security makes a specific determination to the FCC that a given UAS or class of UAS does not pose such risks and UAS critical components produced in a foreign country pose an unacceptable risk to the national security of the United States and to the safety and security of U.S. persons and should be included on the FCC's Covered List, unless the Department of War or the Department of Homeland Security makes a specific determination to the FCC that a given UAS critical component does not pose such risks. The determination also included all communications and video surveillance equipment and services listed in Section 1709(a)(1) of the FY25 National Defense Authorization Act (Pub. L. 118-159).[7]

The Covered List. We find that the National Security Determination constitutes a specific determination of an unacceptable risk to the national security of the United States or the security or safety of United States persons pursuant to section 2 of the Secure Networks Act and subsection 1709(a)(1) of the FY2025 NDAA.[8] Therefore, we conclude that the Commission is required to place the equipment and services in this determination on the Covered List.[9] We update the Covered List to include: "UAS and UAS critical components produced in a foreign country and all communications and video surveillance

[6] National Security Determination at 2.

[7] *Id*.

[8] Although section 1709 requires a determination by an "appropriate national security agency," rather than an Executive Branch interagency body, this determination satisfies the law because several appropriate national security agencies concurred in this determination. *See* Letter from Lee Licata, Deputy Section Chief for Telecom and Supply Chain, Foreign Investment Review Section, National Security Division, U.S. Department of Justice, to Marlene H. Dortch, Secretary, Federal Communications Commission (Sept. 15, 2022) (on file in WC Docket No. 18-89, ET Docket No. 21-232, EA Docket No. 21-233).

[9] Secure Networks Act, 47 U.S.C. § 1601(b)-(d); FY2025 NDAA at § 1709(b)(1)(A). Consistent with the Commission's conclusion in the *Supply Chain Second Report and Order* under the Secure Networks Act, 35 FCC Rcd at 14324-25, para. 91, we find that FY2025 NDAA section 1709 does not give the Commission discretion either to not make any updates to the Covered List if the statutory conditions are satisfied or to make any updates under that statute outside of determinations made by the specified agencies.

equipment and services listed in Section 1709(a)(1) of the FY25 National Defense Authorization Act (Pub. L. 118-159)."[10] If we receive a further specific determination from the Department of War or the Department of Homeland Security that a given UAS, class of UAS, or UAS critical component does not pose unacceptable risks, we will further update the Covered List.

PSHSB takes this action under its authority and obligation to publish and maintain the Covered List. Sections 1.50002(a) and 1.50003 of the Commission's rules require PSHSB to publish the Covered List on the Commission's website, to maintain and update the Covered List, and to monitor the status of determinations.[11]

Equipment Authorization Impacts of the Covered List. Under the Commission's existing rules in section 2.903(a), once added to the Covered List, "covered" equipment is prohibited from receiving equipment authorizations.[12] Moreover, pursuant to section 2.911 of the Commission's rules, all applicants seeking equipment authorization from the Commission must certify that the equipment is not prohibited from receiving an equipment authorization by virtue of being "covered equipment."[13] By so certifying, the applicant would be certifying that the equipment does not qualify as equipment listed in this Notice as "covered." With the exception of the determination concerning FY2025 NDAA section 1709, we clarify that these updates will not implicate various rules and programs applicable to entities "identified" on the Covered List, because this newly-covered equipment is identified by place of production, not by entity.[14]

The updated Covered List is attached as Appendix A to this Public Notice and is also found on the Bureau's website at https://www.fcc.gov/supplychain/coveredlist. [15]

We note the continued availability of FCC staff guidance pursuant to sections 0.191 and 0.31(i) of the Commission's rules. Commission staff will provide guidance to TCBs, test labs, and equipment authorization applicants on the impact of these updates.

For further information, please contact Chris Smeenk, Attorney Adviser, Operations and Emergency Management Division, Public Safety and Homeland Security Bureau, at 202-418-1630 or Chris.Smeenk@fcc.gov.

– FCC –

[10] *See* Appendix A.

[11] 47 CFR §§ 1.50002(a), 1.50003. *See Supply Chain Second Report and Order*, 35 FCC Rcd 14317, 14319, 14325, paras. 72, 77, 92.

[12] 47 CFR § 2.903(a).

[13] 47 CFR § 2.911(d)(5)(i).

[14] *See* 47 CFR §§ 2.903, 2.906, 2.907, 2.911, 2.929, 2.932, 2.938, 2.1033, 2.1043.

[15] The FCC website also contains a list of certain affiliates and subsidiaries of entities identified on the Covered List. The list of affiliates and subsidiaries does not constitute a comprehensive list of all entities that the Commission may find, upon further examination, to qualify as relevant subsidiaries or affiliates of entities on the Covered List. Those entities, whether or not they currently provide covered communications equipment or services, are subject to the Commission's prohibitions, such as the prohibition against obtaining authorizations for covered equipment. *See* Reminder: Communications Equipment And Services On The Covered List Pose An Unacceptable Risk To National Security, *National Security Advisory No. 2025-01, DA 25-927,* note 3 (released October 14, 2025).

APPENDIX A

COVERED LIST (Updated December 22, 2025)*†

Covered Equipment or Services*	Date of Inclusion on Covered List
Telecommunications equipment produced or provided by **Huawei Technologies Company**, including telecommunications or video surveillance services produced or provided by such entity or using such equipment.	March 12, 2021
Telecommunications equipment produced or provided by **ZTE Corporation**, including telecommunications or video surveillance services provided or provided by such entity or using such equipment.	March 12, 2021
Video surveillance and telecommunications equipment produced or provided by **Hytera Communications Corporation**, to the extent it is used for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes, including telecommunications or video surveillance services produced or provided by such entity or using such equipment.	March 12, 2021
Video surveillance and telecommunications equipment produced or provided by **Hangzhou Hikvision Digital Technology Company**, to the extent it is used for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes, including telecommunications or video surveillance services produced or provided by such entity or using such equipment.	March 12, 2021
Video surveillance and telecommunications equipment produced or provided by **Dahua Technology Company**, to the extent it is used for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes, including telecommunications or video surveillance services produced or provided by such entity or using such equipment.	March 12, 2021
Information security products, solutions, and services supplied, directly or indirectly, by **AO Kaspersky Lab** or any of its predecessors, successors, parents, subsidiaries, or affiliates.	March 25, 2022
International telecommunications services provided by **China Mobile International USA Inc.** subject to section 214 of the Communications Act of 1934.	March 25, 2022
Telecommunications services provided by **China Telecom (Americas) Corp.** subject to section 214 of the Communications Act of 1934.	March 25, 2022
International telecommunications services provided by **Pacific Networks Corp.** and its wholly-owned subsidiary **ComNet (USA) LLC** subject to section 214 of the Communications Act of 1934.	September 20, 2022
International telecommunications services provided by **China Unicom (Americas) Operations Limited** subject to section 214 of the Communications Act of 1934.	September 20, 2022
Cybersecurity and anti-virus software produced or provided by **Kaspersky Lab, Inc.** or any of its successors and assignees.	July 23, 2024
Uncrewed aircraft systems (UAS) and UAS critical components produced in a foreign countryδ and all communications and video surveillance equipment and services listed in Section 1709(a)(1) of the FY25 National Defense Authorization Act (Pub. L. 118-159).	December 22, 2025

*The inclusion of producers or providers of equipment or services named on this list should be read to include the subsidiaries and affiliates of such entities.

†Where equipment or services on the list are identified by category, such category should be construed to include only equipment or services capable of the functions outlined in sections 2(b)(2)(A), (B), or (C) of the Secure and Trusted Communications Networks Act of 2019, 47 U.S.C. § 1601(b)(2)(A)-(C).

δ For purposes of inclusion of UAS and UAS critical components, we incorporate the definitions included in the associated National Security Determination.

APPENDIX B

National Security Determination on the Threat Posed by Uncrewed Aircraft Systems (UAS) and UAS Critical Components Produced in Foreign Countries

December 21, 2025

Summary of Determination:

As President Trump noted in the Restoring American Airspace Sovereignty Executive Order (E.O.): "Unmanned aircraft systems (UAS) otherwise known as drones, offer the potential to enhance public safety as well as cement America's leadership in global innovation. But criminals, terrorists, and hostile foreign actors have intensified their weaponization of these technologies, creating new and serious threats to our homeland. Drug cartels use UAS to smuggle fentanyl across our borders, deliver contraband into prisons, surveil law enforcement, and otherwise endanger the public. Mass gatherings are vulnerable to disruptions and threats by unauthorized UAS flights. Critical infrastructure, including military bases, is subject to frequent — and often unidentified — UAS incursions. Immediate action is needed to ensure American sovereignty over its skies and that its airspace remains safe and secure."[16]

The United States is preparing to host several major mass gathering events to include the FIFA World Cup, America250 celebrations, and the Olympic and Paralympic Games. These events will involve unprecedented numbers of spectators, critical infrastructure nodes, and other high value targets in dense urban areas. The Cybersecurity and Infrastructure Security Agency (CISA) and other federal partners have stated that UAS are a routine part of the threat landscape for soft targets and crowded places.[17] Protecting these events is among the highest national security priorities for the United States. To that end, the federal government has created new task forces and grant programs focused specifically on counter UAS protection of host cities and venues, and in the FY26 National Defense Authorization Act Congress established new counter-UAS authorities for state and local law enforcement.[18]

President Trump also established, through the Unleashing American Drone Dominance E.O., that the United States must have a secure and strong domestic UAS industrial base.[19] Additionally, as the President's National Security Strategy (NSS) outlines, it is a national security imperative that we have a resilient industrial base specifically for dual-use technology like UAS. The NSS states, "We want the world's most robust industrial base. American national power depends on a strong industrial sector capable of meeting both peacetime and wartime production demands. That requires not only direct defense industrial production capacity but also

[16] Executive Order 14305, "Restoring American Airspace Sovereignty," June 2025, https://www.whitehouse.gov/presidential-actions/2025/06/restoring-american-airspace-sovereignty/.

[17] U.S. Department of Homeland Security. "Protecting Against the Threat of Unmanned Aircraft Systems." November 2020. https://shorturl.at/IhNSf; U.S. Cybersecurity and Infrastructure Security Agency. "CISA Urges Critical Infrastructure to Be Air Aware." November 2025. https://shorturl.at/B8Okl; and Guggenheim, Benjamin. Politico. "White House presses Congress for drone powers ahead of World Cup, Olympics." November 2025. https://www.politico.com/news/2025/11/26/white-house-asks-congress-for-power-to-take-down-drones-00670564

[18] U.S. Federal Emergency Management Agency. "Notice of Funding Opportunity, FIFA World Cup." November 2025. https://shorturl.at/5UhXS; U.S. Federal Emergency Management Agency. "Counter Unmanned Aircraft Systems Grant Programs." November 2025. https://shorturl.at/4wkaw; National Defense Authorization Act for Fiscal Year 2026, Pub. L. No. 119-60 § 8601 – 8607.

[19] Executive Order 14307. "Unleashing American Drone Dominance" June 2025. https://www.whitehouse.gov/presidential-actions/2025/06/unleashing-american-drone-dominance/

defense-related production capacity. Cultivating American industrial strength must become the highest priority of national economic policy."[20] Relying on UAS and UAS critical components produced in foreign countries poses an unacceptable national security risk to the United States. To ensure American companies are able to meet both peacetime and wartime demand, the U.S. UAS industry cannot rely on foreign-produced UAS critical components.

In order to fulfill the purpose of the Restoring American Airspace Sovereignty E.O., the Unleashing American Drone Dominance E.O., and the NSS, UAS and UAS critical components must be produced in the United States. This will reduce the risk of direct UAS attacks and disruptions, unauthorized surveillance, sensitive data exfiltration, and other UAS threats to the homeland. Furthermore, it will ensure our domestic UAS and UAS critical component manufacturing is resilient and independent, a critical national security imperative. UAS are inherently dual-use: they are both commercial platforms and potentially military or paramilitary sensors and weapons. UAS and UAS critical components, including data transmission devices, communications systems, flight controllers, ground control stations, controllers, navigation systems, batteries, smart batteries, and motors produced in a foreign country could enable persistent surveillance, data exfiltration, and destructive operations over U.S. territory, including over World Cup and Olympic venues and other mass gathering events. U.S. cybersecurity and critical infrastructure guidance has repeatedly highlighted how foreign manufactured UAS can be used to harvest sensitive data, used to enable remote unauthorized access, or disabled at will via software updates.[21]

In response to this threat, the White House convened an executive branch interagency body with appropriate national security expertise, *see* 47 U.S.C. § 1601(c)(1), including appropriate national security agencies, *id*. § 1601(c)(4). This body determined that UAS produced in a foreign country pose an unacceptable risk to the national security of the United States and to the safety and security of U.S. persons and should be included on the FCC's Covered List, unless the Department of War or the Department of Homeland Security makes a specific determination to the FCC that a given UAS or class of UAS does not pose such risks.[22] This body also determined that UAS critical components produced in a foreign country pose an unacceptable risk to the national security of the United States and to the safety and security of U.S. persons and should be included on the FCC's Covered List, unless the Department of War or the Department of Homeland Security makes a specific determination to the FCC that a given UAS critical component does not pose such risks. These determinations included all communications and video surveillance equipment and services listed in Section 1709(a)(1) of the FY25 National Defense Authorization Act.[23] The interagency group determined that UAS and UAS critical components produced in a foreign country pose unacceptable risks, given the threats from unauthorized surveillance, sensitive data exfiltration, supply chain vulnerabilities, and other potential threats to the homeland.

[20] "National Security Strategy of the United States of America." November 2025. https://www.whitehouse.gov/wp-content/uploads/2025/12/2025-National-Security-Strategy.pdf

[21] U.S. Cybersecurity and Infrastructure Security Agency. "Release Cybersecurity Guidance on Chinese-Manufactured UAS for Critical Infrastructure Owners and Operators." January 2024. https://tinyurl.com/mpn5zfyk ; and U.S. Cybersecurity and Infrastructure Security Agency. "Be Air Aware." Access December 2025. https://www.cisa.gov/topics/physical-security/be-air-aware/uas-cybersecurity

[22] 47 U.S.C. § 1601(c).

[23] Servicemember Quality of Life Improvement and National Defense Authorization Act for Fiscal Year 2025, Pub. L. No. 118-159, § 1709, 138 Stat. 1773, 2209-10 (2024) (FY2025 NDAA).

Summary of Supporting Evidence:

Federal planning for the 2026 FIFA World Cup and 2028 Olympics already assumes that UAS will be a central threat vector. CISA's soft-target and UAS guidance notes that crowded venues, transportation nodes, and public-gathering areas are particularly vulnerable to hostile drone activity.[24] Recent congressional hearings on mass-gathering security have emphasized that UAS are now a routine part of incident planning, alongside more traditional threats.[25] The Federal Emergency Management Agency, the Department of Homeland Security, and the Department of War are already investing heavily in detection, tracking, and mitigation capabilities with these specific events in mind.[26] UAS are also playing a critical enabling role on the battlefield in many modern conflicts. In Ukraine and Israel-Gaza, low-cost commercial UAS inflict extensive damage and have caused significant loss of life.[27] Drug Cartels are also reportedly using foreign-produced UAS to smuggle drugs into the United States and carry out attacks.[28]

President Trump's Unleashing American Drone Dominance E.O. establishes that it is the policy of the United States to establish a resilient and strong American drone industrial base. In order to achieve this goal, we must cease the importation of all new foreign-manufactured UAS and UAS critical components.[29] Additionally, President Trump's Restoring American Airspace Sovereignty E.O. calls for the United States to "scale up domestic production and expand the export of trusted, American-manufactured drone technologies to global markets."[30] Given the increasing importance of UAS to U.S. warfighters, first responders, and business owners, it is critical to U.S. national security that the United States has domestic supply of UAS, made with U.S.-produced critical components.

Permitting UAS critical components from foreign countries into the United States undermines the resiliency of our UAS industrial base, increases the risk to our national airspace, and creates a potential for large-scale attacks during large gatherings. Even when marketed as "commercial" or "recreational," certain legal regimes in foreign countries can compel entities to provide real-time telemetry, imagery, and location data above U.S. soil, or to change the UAS behavior via remote software updates.[31] This poses clear risks that foreign countries could leverage UAS produced with critical components made in a foreign country to engage in intelligence collection, acts of terrorism, attacks on critical infrastructure in the U.S. homeland, or massive supply chain disruption.

---

[24] U.S. Cybersecurity and Infrastructure Security Agency. "Securing Public Gatherings." https://tinyurl.com/32ekm9s2

[25] U.S. House of Representatives Committee on Homeland Security. "Mass Gathering Events: Assessing Security Coordination and Preparedness." May 2025. https://tinyurl.com/3wcjpa9d

[26] *Supra* note 2.

[27] Newman, Marissa. Bloomberg. "Hamas's Cheap, Makeshift Drones Are Outsmarting Israel's High-Tech military." December 2023. https://www.bloomberg.com/news/articles/2023-12-19/israel-s-advanced-defenses-are-pierced-by-makeshift-hamas-drones-in-gaza-war

Brown, Steve. Kyiv Post. "ANALYSIS: Casualty Figures Reveal Game-Changing Impact of Drones on Ukrainian Battlefield." March 2025. https://www.kyivpost.com/analysis/49712

[28] Ziemer, Henry. Center for Strategic & International Studies. "The United States Needs a Southwest Drone Wall." December 2025. https://shorturl.at/GpKQr

[29] Executive Order 14307. "Unleashing American Drone Dominance" June 2025. https://www.whitehouse.gov/presidential-actions/2025/06/unleashing-american-drone-dominance/

[30] *Supra* note 1.

[31] *Supra* note 6.

Furthermore, the opaque supply chains for UAS manufactured in foreign countries can prevent the U.S. government from conducting due diligence to ensure compliance with certain standards. NIST's supply‐chain risk‐management guidance emphasizes that organizations must account for the provenance, update pathways, and support arrangements of Information and Communication Technology (ICT)‐enabled products, including those embedded in physical systems like UAS.[32] Given the nature of legal regimes in certain foreign countries, the U.S. government has no assurance that those states will not withhold updates, tamper with specific devices, or subtly degrade the performance of UAS or UAS critical components imported into the United States.

Given these facts and assessments, in the context of World Cup and Olympic security and the growing need to protect U.S. airspace from cartels, terrorist groups, and foreign governments seeking to collect intelligence on U.S. soil, the U.S. government has clear national security concerns that entities subject to the jurisdiction of foreign countries, including those listed in Sec. 1709 of the FY25 NDAA, could leverage their roles as the producer of a UAS or UAS critical component to directly harm U.S. persons. Such incidents could include: disabling fleets of ostensibly commercial drones used by U.S. public‐safety agencies, coordinating swarms of privately owned UAS for disruptive or coercive effect, or leveraging data collected by the UAS platform to conduct surveillance or intelligence operations.

As a result and per the reasons summarized in this document, the U.S. government's executive branch interagency body is referring to the FCC's Covered List all UAS produced in a foreign country, unless the Department of War or Department of Homeland Security makes a specific determination to the FCC that a given UAS or class of UAS does not pose such risks. This body also determined that UAS critical components produced in a foreign country pose an unacceptable risk to the national security of the United States and to the safety and security of U.S. persons and should be included on the FCC's Covered List, unless the Department of War or Department of Homeland Security makes a specific determination to the FCC that a given UAS critical component does not pose such risks. These determinations include all video surveillance and communications equipment in Section 1709 of the FY25 NDAA. This action is necessary to protect the homeland, Unleash American Drone Dominance, and Restore American Airspace Sovereignty.

Definitions:

FCC: For the purpose of this determination, the term "FCC" shall mean the Federal Communications Commission.

Uncrewed Aircraft (UA): For the purpose of this determination, the term "uncrewed aircraft (UA)" has the meaning found in 47 CFR 88.5: *An aircraft operated without the possibility of direct human intervention from within or on the aircraft.*

Uncrewed Aircraft System (UAS): For the purpose of this determination, the term "uncrewed aircraft system (UAS)" has the meaning found in 47 CFR 88.5: *An Uncrewed Aircraft and its associated elements (including an uncrewed aircraft station, communication links, and the*

[32] National Institute for Standards and Technology. "Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations." May 2022. https://csrc.nist.gov/pubs/sp/800/161/r1/final

components not on board the UA that control the UA) that are required for the safe and efficient operation of the UA in the airspace of the United States.

UAS Critical Components: For the purpose of this determination, the term "UAS critical components" includes but is not limited to the following UAS components and any associated software:

- Data transmission devices
- Communications systems
- Flight controllers
- Ground control stations and UAS controllers
- Navigation systems
- Sensors and Cameras
- Batteries and Battery Management Systems
- Motors