PUBLIC NOTICE

Federal Communications Commission
45 L Street NE
Washington, DC 20554

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

DA 26-278
Released: March 23, 2026

FCC'S PUBLIC SAFETY AND HOMELAND SECURITY BUREAU ANNOUNCES ADDITION OF ROUTERS PRODUCED IN FOREIGN COUNTRIES 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] and sections 1.50002(a) and 1.50003 of the Commission's rules,[3] PSHSB announces the addition of routers produced in a foreign country to the Covered List. We make this addition 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.[4]

National Security Determination. On March 20, 2026, the FCC received a National Security Determination regarding the unacceptable risks posed by routers produced in foreign countries. Among other points, the National Security Determination states:

> "Recently, malicious state and non-state sponsored cyber attackers have increasingly leveraged the vulnerabilities in small and home office routers produced abroad to carry out direct attacks against American civilians in their homes. From disrupting network connectivity to enabling local networking espionage and intellectual property theft, foreign-produced routers present unacceptable risks to Americans. Additionally, routers produced abroad were directly implicated in the

[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 Mar. 18, 2026).

[2] 47 U.S.C. § 1601.

[3] 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*).

[4] *See* 47 U.S.C. § 1601(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 C to this Public Notice.

> Volt, Flax, and Salt Typhoon cyberattacks which targeted critical American communications, energy, transportation, and water infrastructure. Routers in the United States must have trusted supply chains so we are not providing foreign actors with a built-in backdoor to American homes, businesses, critical infrastructure, and emergency services."[5]

As a result of the threats described in the National Security Determination, the Executive Branch interagency body determined that routers produced in foreign countries, regardless of nationality of the producer, pose the following unacceptable risks to the United States: "(1) introducing a supply chain vulnerability that could disrupt the U.S. economy, critical infrastructure, and national defense; and (2) establishing a severe cybersecurity risk that could be leveraged to immediately and severely disrupt U.S. critical infrastructure and directly harm U.S. persons."[6]

Based on these findings, the Executive Branch interagency body, including several appropriate national security agencies, concluded that 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: Routers produced in a foreign country, unless the Department of War (DoW) or the Department of Homeland Security (DHS) transmits to the FCC a specific determination that a given router or class of routers does not pose such risks.[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.[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:

> "Routers produced in a foreign country, except routers which have been granted a Conditional Approval by DoW or DHS."

Conditional Approvals. The Executive Branch interagency body has established a process in which entities producing routers in a foreign country can request DoW and DHS to evaluate whether their routers do not pose unacceptable risks to national security and receive Conditional Approvals that would exempt the routers from the Covered List. Guidance on submissions for Conditional Approvals is found in Annex A to the National Security Determination.[10]

If we receive a further specific determination from the DoW or DHS that a given router or class of routers 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

[5] National Security Determination at 1-2 (internal citations omitted).

[6] *Id.* at 2.

[7] *Id.* at 2.

[8] 47 U.S.C. § 1601(c).

[9] 47 U.S.C. § 1601(b)-(d).

[10] Annex A to the National Security Determination can be found in Appendix C to this Public Notice.

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 applications 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 Public Notice as "covered." 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 and the list of devices that have received Conditional Approvals are attached as Appendices A and B to this Public Notice and are also located 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 Rebecca Clinton at Rebecca.Clinton@fcc.gov or 202-418-7815, or Chris Smeenk at Chris.Smeenk@fcc.gov or 202-418-1630, Attorney Advisors, Operations and Emergency Management Division, Public Safety and Homeland Security Bureau.

[11] 47 CFR §§ 1.50002(a), 1.50003. *See Supply Chain Second Report and Order*, 35 FCC Rcd at 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 (PSHSB Oct. 14, 2025).

APPENDIX A

COVERED LIST (Updated March 23, 2026)*†

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 country††—except (a) UAS and UAS critical components included on the Defense Contract Management Agency's (DCMA's) Blue UAS Cleared List, until January 1, 2027,# (b) UAS critical components that qualify as "domestic end products" under the Buy American Standard, 48 CFR 25.101(a), until January 1, 2027; and (c) devices which have been granted a Conditional Approval by DoW or DHS—and all communications and video surveillance equipment and services	December 22, 2025 Updated: January 7, 2026 Updated: March 18, 2026

listed in Section 1709(a)(1) of the FY25 National Defense Authorization Act (Pub. L. 118-159).	
Routers^ produced in a foreign country, except routers which have been granted a Conditional Approval by DoW or DHS.	March 23, 2026

*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).

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

#The "Blue UAS list" referred to in the National Security Determination is the combination of the "Blue UAS Cleared List" at https://bluelist.appsplatformportals.us/Cleared-List/ and the list of compliant UAS components and software at https://bluelist.appsplatformportals.us/Framework/. We use the term "Blue UAS Cleared List" to refer to both lists.

^For purposes of inclusion of routers, we incorporate the definitions included in the associated National Security Determination.

APPENDIX B

Conditional Approvals

March 18, 2026

Devices Granted Conditional Approval	Date of Conditional Approval
SiFly Aviation, Inc. Q12 Uncrewed Aircraft System	March 17, 2026-December 31, 2026
Mobilicom SkyHopper Series / M Band / Tactical Data Link, Various Controllers, and ICE, OS3 Security Software	March 17, 2026-December 31, 2026
ScoutDI Scout 137 Uncrewed Aircraft System	March 17, 2026-December 31, 2026
Verge, Inc. X1 Uncrewed Aircraft System	March 17, 2026-December 31, 2026

APPENDIX C

National Security Determination on the Threat Posed by Routers Produced by Foreign Countries

March 20, 2026

Summary of Determination:

The President's 2025 National Security Strategy (NSS) says, "the United States must never be dependent on any outside power for core components—from raw materials to parts to finished products—necessary to the nation's defense or economy. We must re-secure our own independent and reliable access to the goods we need to defend ourselves and preserve our way of life."[1] One of these core components that is necessary to both our nation's defense and economy is routers. Routers are the key networking device that enable American homes, schools, businesses, critical infrastructure providers, and emergency services to connect to the internet every day. A majority of the routers currently in Americans' homes and businesses are manufactured in foreign countries.[2] Given the criticality of routers to the successful functioning of our nation's economy and defense, the United States can no longer depend on foreign nations for router manufacturing.

Ninety-six percent of Americans use the internet and routers serve as a primary means for internet access.[3] Routers are critical networking devices that manage the flow of data and information between connected devices. Americans rely on routers for secure, reliable, and efficient communications across an expanding digital landscape. Secure and dependable routers enable Americans to have consistent, stable, and reliable connection to the internet which is critical for maintaining functional communications, critical infrastructure, and emergency services.

Compromised routers can enable in-depth network surveillance, data exfiltration, botnet attacks, and unauthorized access to U.S. government or American businesses' networks.[4] The United States must have secure and trusted routers. However, currently a majority of the routers in American homes and businesses are produced outside of the United States.[5] Allowing routers produced abroad to dominate the U.S. market creates unacceptable economic, national security, and cybersecurity risks.

Recently, malicious state and non-state sponsored cyber attackers have increasingly leveraged the vulnerabilities in small and home office routers produced abroad to carry out direct attacks

[1] "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
[2] "US conducting criminal antitrust investigation into TP-Link, Bloomberg News reports." Reuters. April 2025. https://www.reuters.com/technology/tp-link-faces-us-criminal-antitrust-investigation-bloomberg-news-reports-2025-04-25/
[3] "Internet, Broadband Fact Sheet." Pew Research Center. November 2025. https://www.pewresearch.org/internet/fact-sheet/internet-broadband/
[4] "Recommended Cybersecurity Requirements for Consumer-Grade Router Products." National Institute of Standards and Technology. September 2024. https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8425A.pdf
[5] "U.S. Weighs Ban on Chinese-Made Router in Millions of American Homes." Wall Street Journal. December 2024. https://www.wsj.com/politics/national-security/us-ban-china-router-tp-link-systems-7d7507e6

against American civilians in their homes. [6] From disrupting network connectivity to enabling local networking espionage and intellectual property theft, foreign-produced routers present additional and unacceptable risks to Americans. Additionally, routers produced abroad were directly implicated in the Volt, Flax, and Salt Typhoon cyberattacks which targeted critical American communications, energy, transportation, and water infrastructure.[7][8] Routers in the United States must have trusted supply chains so we are not providing foreign actors with potential built-in backdoors to American homes, businesses, critical infrastructure, and emergency services.

To address the threat from routers produced abroad, the White House convened an executive branch interagency body with appropriate national security expertise, *see* 47 U.S.C. § 1601(c)(1), comprising agencies that included appropriate national security agencies, *id*. § 1601(c)(4) which determined jointly and severally that routers produced in a foreign country, regardless of the nationality of the producer, 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 (DoW) or the Department of Homeland Security (DHS) transmits to the FCC a specific determination that a given router or class of routers do not pose such risks. The interagency body determined that foreign produced routers posed the following unacceptable risks to the United States: (1) introducing a supply chain vulnerability that could disrupt the U.S. economy, critical infrastructure, and national defense; and (2) establishing a severe cybersecurity risk that could be leveraged to immediately and severely disrupt U.S. critical infrastructure and directly harm U.S. persons. Production generally includes any major stage of the process through which the device is made, including manufacturing, assembly, design, and development.

To facilitate this transition period, entities that produce routers in a foreign country are encouraged to apply for Conditional Approvals (Annex A) which, if approved, will allow such producers to continue to receive FCC authorization for their products while they work to address the U.S. government's national security concerns described above.

Summary of Supporting Evidence:

According to a 2024 National Institute of Standards and Technology publication, "A compromised router opens the door to a host of potential exploited vulnerabilities and impacts, ranging from unauthorized access and sensitive information dissemination to the possibility of malicious attacks on connected devices. Ensuring the security of routers is crucial for

[6] "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure." Cybersecurity and Infrastructure Agency. February 2024. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

[7] "Joint Cybersecurity Advisory: People's Republic of China-Linked Actors Compromise Routers and IoT Devices for Botnet Operations." September 2024. https://media.defense.gov/2024/Sep/18/2003547016/-1/-1/0/CSA-PRC-LINKED-ACTORS-BOTNET.PDF

[8] "Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System." September 2025. https://www.cisa.gov/sites/default/files/2025-09/CSA_COUNTERING_CHINA_STATE_ACTORS_COMPROMISE_OF_NETWORKS.pdf

safeguarding not only individual privacy and safety but also the integrity and availability of entire networks."[9]

Unsecure and foreign-produced routers are prime targets for attackers and have been used in multiple recent cyberattacks to enable hackers to gain access to networks and use them as launching pads to compromise critical infrastructure. The Cybersecurity and Infrastructure Agency has labeled edge networking devices, including routers, as the "attack-vector of choice" for hackers and cybercriminals.[10] In Salt Typhoon attacks, state-sponsored cyber threat actors leveraged compromised and foreign-produced routers to jump to embed and gain long term access to certain networks and pivot to others depending on their target.[11] As CISA wrote in a September 2025 Cybersecurity Advisory, Advanced Persistent Threat (APT) actors are "modifying router configurations for lateral movement pivoting between networks and using virtualized containers on network devices to evade detection."[12] This allows APTs to find and target critical networks such as telecommunications, government, transportation, lodging, and military infrastructure networks.

Additionally, in September 2024, the Federal Bureau of Investigation (FBI), Cyber National Mission Force (CNMF), and National Security Agency (NSA) published a joint cybersecurity assessment outlining how cyber actors have compromised foreign-produced routers to create "a network of compromised nodes (a "botnet") positioned for malicious activity. The actors may then use the botnet as a proxy to conceal their identities while deploying distributed denial of service (DDoS) attacks or compromising targeted U.S. networks."[13] Unsecure foreign-produced routers in homes and American businesses are enabling hackers to create massive networks that can be leveraged to carry out password spraying, unauthorized network access, and act as proxies for espionage.

In October 2024, Microsoft publicly announced that for over a year the company had observed cyber actors targeting and stealing information from Microsoft customers enabled by highly evasive password spray attacks. Microsoft tracked the attack to compromised routers that were produced outside of the United States. The APT actors exploited a vulnerability in the routers to gain remote code execution capability and Microsoft assessed that multiple APTs were exploiting similar vulnerabilities to carry out attacks.[14] This expansive attack targeted organizations in North America and Europe, including government agencies, non-governmental

[9] "Recommended Cybersecurity Requirements for Consumer-Grade Router Products." National Institute of Standards and Technology. September 2024. https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8425A.pdf
[10] "The Increasing Threat to Network Infrastructure Devices and Recommended Mitigations" CISA. September 2016. https://www.cisa.gov/news-events/alerts/2016/09/06/increasing-threat-network-infrastructure-devices-and-recommended-mitigations
[11] "Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System." September 2025. https://www.cisa.gov/sites/default/files/2025-09/CSA_COUNTERING_CHINA_STATE_ACTORS_COMPROMISE_OF_NETWORKS.pdf
[12] Ibid
[13] "Joint Cybersecurity Advisory: People's Republic of China-Linked Actors Compromise Routers and IoT Devices for Botnet Operations." September 2024. https://media.defense.gov/2024/Sep/18/2003547016/-1/-1/0/CSA-PRC-LINKED-ACTORS-BOTNET.PDF
[14] "Chinese threat actor Storm-0940 uses credentials from password spray attacks from a covert network." Microsoft. October 2024. https://www.microsoft.com/en-us/security/blog/2024/10/31/chinese-threat-actor-storm-0940-uses-credentials-from-password-spray-attacks-from-a-covert-network/

organizations, think tanks, law firms, energy firms, IT providers, and defense industrial base entities.[15]

The vulnerabilities introduced into American networks and critical infrastructure resulting from foreign-manufactured routers is unacceptable. To address the threat from routers produced abroad, the White House convened an executive branch interagency body with appropriate national security expertise, *see* 47 U.S.C. § 1601(c)(1), comprising agencies that included appropriate national security agencies, *id*. § 1601(c)(4) which determined jointly and severally that routers produced in a foreign country, regardless of the nationality of the producer, 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 DoW or DHS transmits to the FCC a specific determination that a given router or class of routers do not pose such risks. The interagency body determined that foreign produced routers posed the following unacceptable risks to the United States: (1) introducing a supply chain vulnerability that could disrupt the U.S. economy, critical infrastructure, and national defense; and (2) establishing a severe cybersecurity risk that could be leveraged to immediately and severely disrupt U.S. critical infrastructure and directly harm U.S. persons. Production generally includes any major stage of the process through which the device is made, including manufacturing, assembly, design, and development.

Definitions:

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

Routers: For the purpose of this determination, the term "Routers" is defined by National Institute of Science and Technology's Internal Report 8425A to include consumer-grade networking devices that are primarily intended for residential use and can be installed by the customer. Routers forward data packets, most commonly Internet Protocol (IP) packets, between networked systems.

[15] "Quad7 Activity" MITRE. October 2025. https://attack.mitre.org/campaigns/C0055/

Annex A: Guidance on Submissions for Conditional Approval for Routers Produced by Foreign Countries Subject to the FCC's Covered List

March 20, 2026

Background

On March 20, 2026, the FCC updated the Covered List to include "Routers produced by foreign countries," which resulted in such "covered" equipment being prohibited from receiving an equipment authorization from the FCC unless the Department of War (DoW) or DHS makes a specific determination to the FCC that a given router or class of routers (e.g., routers produced by a specified entity) do not pose unacceptable risks to the national security of the United States or to the safety and security of U.S. persons. This document provides guidance for producers of routers covered by this action to apply for a Conditional Approval, through an individualized assessment of "unacceptable risks" that would exempt the approved entity from restrictions imposed by inclusion on the FCC's Covered List. To be considered for Conditional Approval from DoW or DHS, router producers must submit the information requested in this document. This information will enable DoW and DHS to assess national security risks, supply chain resilience, and the applicant's commitment to establishing trusted manufacturing capacity in the United States to ultimately judge whether the router producer poses "unacceptable risks." Submission does not guarantee approval. DoW and DHS may request additional information as necessary. All decisions are final and can only be adjusted at the discretion of DoW and DHS.

Information Requested

Any entity that is seeking a Conditional Approval must provide the information requested in this document. Failure to provide all the requested information may result in delays or denial of the application. Submissions must include a certification by an authorized corporate officer that all the information is complete, accurate and that any material change will be promptly disclosed. Applicants that knowingly violate the terms of the Conditional Approval or materially misrepresent information provided to the U.S. Government will have their Conditional Approval terminated (if granted) and will be precluded from applying again. Conditional Approvals will be granted for periods of up to 18 months.

1. **Corporate Structure:**
    a. Legal name, jurisdiction(s) of incorporation, and principal place of business;
    b. Complete ownership structure, including parents, subsidiaries, affiliates, and joint ventures;
    c. Beneficial owners holding five percent or greater equity;
    d. Board members and executive leadership, including nationality and country of residence; and
    e. Any foreign government ownership, control, influence, financing, or material support (applicants must identify any arrangements that allow foreign persons or governments to influence operations, decision-making, or access to technology.)

2. **Manufacturing and Supply Chain Disclosure:**
    a. A detailed bill of materials for the router for which the applicant is seeking the Conditional Approval;

b. Country of origin for all components in the router and country of origin for the design of the router;
c. Entities responsible for IP ownership and software updates for the router;
d. Justification on why any foreign manufactured router is not currently manufactured in the United States, including why these foreign sources were selected and whether alternatives exist;
e. Locations of manufacturing, final assembly, and testing for the router for which the applicant is seeking the Conditional Approval;
f. Country of origin for any onboard software and firmware;
g. Quantitative assessment of supply chain concentration by country, expressed as both a percentage of total value and production volume; and
h. Identification of any single points of failure in the supply chain for the router including sole source suppliers, the country of those sole-source suppliers, and a description of contingency plans if those suppliers become unavailable.

3. **U.S. Manufacturing and Onshoring Plan**
   a. A detailed, time-bound plan to establish or expand manufacturing in the United States for the router for which the applicant is seeking Conditional Approval in order for that device to qualify for FCC authorization;
   b. A dedicated point of contact or office responsible for implementing and overseeing the U.S. manufacturing and onshoring plan. This individual or office must provide the agency issuing the Conditional Approval an update on the status of their onshoring plan once a quarter;
   c. A description of existing U.S.-based manufacturing and assembly for the router including: percentage of components assembled in the United States and current U.S. headcount and facilities (locations, functions, etc.);
   d. A description of committed and planned capital expenditures, financing, or other investments dedicated to U.S.-based manufacturing and assembly over the next 1-5 years, including expected timelines and milestones; and
   e. An inventory of the progress made on the U.S. manufacturing and onshoring plans submitted for all previous covered approvals, if applying for an extension of an existing Conditional Approval or if the applicant has any other existing covered Conditional Approval.

###

For questions regarding FCC's Covered List please contact Chris Smeenk (chris.smeenk@fcc.gov).

For entities seeking Conditional Approval please email: Conditional-approvals@fcc.gov