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/