May 20, 2024

Hon. Mike Johnson
Speaker
U.S. House of Representatives
568 Cannon House Office Building
Washington, DC 20515

Hon. Hakeem Jeffries
Minority Leader
U.S. House of Representatives
2433 Rayburn House Office Building
Washington, DC 2051

Support for the ROUTERS Act

Dear Speaker Johnson and Minority Leader Jeffries,

We, the undersigned organizations and individuals, write in support of the Removing Our Unsecure Technologies to Ensure Reliability and Security (ROUTERS) Act. Specifically, we encourage House leadership to take up the ROUTERS Act posthaste. We further request that the House Appropriations Committee consider including report language in the FY2025 appropriations package encouraging agencies to investigate their information technology (IT) infrastructure and "rip and replace" any hardware manufactured by a company controlled by a foreign adversary nation.

Passed unanimously out of the House Energy and Commerce Committee in March, the ROUTERS Act would require a report from the Department of Commerce informing policymakers of potential risks posed by consumer internet routers, modems, and other technologies produced by companies based in or controlled by foreign adversary nations. To safeguard America's national and economic security, members of Congress need reliable information on technological vulnerabilities in consumer products produced in nations such as China and Russia. The ROUTERS Act would help provide such information.

The Chinese Communist Party and other foreign adversaries have attempted to compromise our national and economic security at all levels of the "tech stack."[1] Congress previously addressed threats to our telecommunications infrastructure by passing the bipartisan Secure Equipment Act, which removed and banned the use of products made by Chinese telecommunications firms Huawei and ZTE. Congress recently addressed

[1] U.S. Department of Justice, "Information About the Department of Justice's China Initiative and a Compilation of China-Related Prosecutions Since 2018," November 19, 2021, https://www.justice.gov/archives/nsd/information-about-department-justice-s-china-initiative-and-compilation-china-related.

threats at the "edge" of the tech stack with legislation that enables the president to force the divestment of foreign-controlled platforms such as TikTok. Congress has requested studies that have helped illustrate the threats posed by the federal government's use of other types of hardware, such as drones manufactured by Chinese-based drone company DJI.[2] But Congress has not yet comprehensively examined the national security and economic vulnerabilities posed by the "middle" sections of our tech stack as represented by routers and modems.

Concerns about potential vulnerabilities in routers and modems are well-founded, and passing the ROUTERS Act will help Congress take appropriate measures to secure our digital infrastructure. In January 2024, CCP-supported hacker groups in Europe exploited vulnerabilities in routers made by the Chinese company TP-Link to conduct cyber espionage operations.[3] The National Institute of Standards and Technology (NIST) has logged hundreds of reports of cybersecurity vulnerabilities within TP-Link's products in its National Vulnerabilities Database.[4] Even with these known vulnerabilities, agencies such as the Department of Defense, the National Aeronautics and Space Administration, and the General Services Administration have reportedly purchased TP-Link hardware.[5]

The ROUTERS Act would begin the process of identifying the level of threat that such technologies pose to American national and economic security. The bill marks another

---

[2] "Warner, Blackburn, Colleagues Request Cybersecurity Analysis of Chinese-Made Drones," Office of Senator Mark Warner, March 16, 2023, https://www.warner.senate.gov/public/index.cfm/2023/3/warner-blackburn-colleagues-request-cybersecurity-analysis-of-chinese-made-drones; "Cybersecurity Guidance: Chinese-Manufactured UAS," Cybersecurity and Information Security Agency, January 17, 2024, https://www.cisa.gov/resources-tools/resources/cybersecurity-guidance-chinese-manufactured-uas.

[3] "Check Point Research Reveals a Malicious Firmware Implant for TP-Link Routers, Linked to Chinese APT Group," Check Point Software Technologies, May 16, 2023, https://blog.checkpoint.com/security/check-point-research-reveals-a-malicious-firmware-implant-for-tp-link-routers-linked-to-chinese-apt-group/.

[4] "National Vulnerability Database," National Institute of Standards and Technology, February 6, 2024, https://nvd.nist.gov/vuln/search/results?isCpeNameSearch=false&query=TP-Link&results_type=overview&form_type=Basic&search_type=all&startIndex=0.

[5] "Spending by Prime Award FY08 - FY24," USAspending.gov, accessed May 2, 2024, https://www.usaspending.gov/search/?hash=095e65af207201c14a0b9d44c4e75dc3.

step in the bipartisan effort to secure our supply chains and tech stack from threats posed by products and vendors based in or beholden to countries of concern.

In addition to taking up the ROUTERS Act, we encourage Congress to include report language in the FY2025 appropriations package that recommends federal agencies conduct an inventory of their routers and remove any hardware manufactured in countries of concern that could have built-in cybersecurity vulnerabilities. Historically, when addressing national security threats to our tech stack, the federal government has led by example, voluntarily removing vulnerable hardware and software from government devices and networks. While, to our knowledge, no legislation has yet been proposed requiring federal agencies to do so, we believe that the appropriations report language this appropriations cycle could kickstart the removal of vulnerable routers and modems from federal IT systems. After the passage of the ROUTERS Act, this would be a great second step toward addressing threats at the highest level and proactively mitigating any potential harm.

Thank you for your consideration and leadership on this vital issue. We look forward to working with you to ensure that this piece of legislation becomes law and to continue the effort to secure our technological infrastructure.

Sincerely,

Zach Graves
Executive Director
Foundation for American Innovation

Nathan Leamer
Executive Director
Digital First Project

Yaël Ossowski
Deputy Director
Consumer Choice Center

Kara Frederick
Director, Tech Policy Center
The Heritage Foundation*

Ajit Pai
Former FCC Chairman
Partner
Searchlight Capital Partners

Joel Thayer
President
Digital Progress Institute

Jonathan Cannon
Policy Counsel, Tech and Innovation
R Street Institute

Matt Stoller
Director of Research
American Economic Liberties Project

James Erwin
Executive Director
Digital Liberty

Dr. Roslyn Layton
Co-Founder
China Tech Threat

Tom Hebert
Executive Director
Open Competition Center

Evan Swartzrauber
Senior Fellow
Foundation for American Innovation

** The Heritage Foundation is listed for identification purposes only. The views are personal and do not reflect an institutional position for The Heritage Foundation or its Board of Trustees.*