119TH CONGRESS
1st Session
HOUSE OF REPRESENTATIVES
REPORT
119–75

REMOVING OUR UNSECURE TECHNOLOGIES TO ENSURE RELIABILITY AND SECURITY ACT

APRIL 24, 2025.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. GUTHRIE, from the Committee on Energy and Commerce, submitted the following

R E P O R T

[To accompany H.R. 866]

The Committee on Energy and Commerce, to whom was referred the bill (H.R. 866) to direct the Secretary of Commerce, acting through the Assistant Secretary of Commerce for Communications and Information, to conduct a study of the national security risks posed by consumer routers, modems, and devices that combine a modem and router, and for other purposes, having considered the same, reports favorably thereon with an amendment and recommends that the bill as amended do pass.

CONTENTS

59–006

The amendment is as follows:

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the "Removing Our Unsecure Technologies to Ensure Reliability and Security Act" or the "ROUTERS Act".

SEC. 2. STUDY OF RISKS POSED BY CERTAIN ROUTERS AND MODEMS.

(a) IN GENERAL.—The Secretary shall conduct a study of the national security risks and cybersecurity vulnerabilities posed by consumer routers, modems, and devices that combine a modem and router that are designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the influence of a covered country.

(b) REPORT TO CONGRESS.—Not later than 1 year after the date of the enactment of this Act, the Secretary shall submit to the Committee on Energy and Commerce of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate a report on the results of the study conducted under subsection (a).

(c) CONSULTATION WITHIN DEPARTMENT.—In conducting the study under subsection (a), the Secretary shall consult with appropriate bureaus and offices within the Department of Commerce.

(d) DEFINITIONS.—In this section:

(1) COVERED COUNTRY.—The term "covered country" means a country specified in section 4872(f)(2) of title 10, United States Code.

(2) SECRETARY.—The term "Secretary" means the Secretary of Commerce, acting through the Assistant Secretary of Commerce for Communications and Information.

PURPOSE AND SUMMARY

H.R. 866, the Removing Our Unsecure Technologies to Ensure Reliability and Security Act, or the ROUTERS Act, was introduced by Representatives Robert E. Latta (R–OH) and Robin L. Kelly (D–IL) on January 31, 2025. It would direct the Secretary of Commerce (Secretary), acting through the Assistant Secretary of Commerce for Communications and Information, to conduct a study on the national security risks and cybersecurity vulnerabilities posed by consumer routers, modems, and combined modem-router devices designed, developed, manufactured, or supplied by entities with ties to foreign adversaries. The Secretary would be required to submit a report to Congress on the findings of this study within one year of the enactment of the Act.

BACKGROUND AND NEED FOR LEGISLATION

Routers and modems are key components of the communications ecosystem. They are the equipment through which users and devices connect to the internet. As a result, they are critical to communications networks and a significant amount of data flows through this equipment.

But routers and modems can include cybersecurity vulnerabilities, opening them up to attacks from bad actors. Indeed, the Cybersecurity and Infrastructure Security Agency (CISA) and the National Institute of Standards and Technology (NIST) have found vulnerabilities in routers that could be exploited for cyberattacks.[1]

[1] Cybersecurity and Infrastructure Security Agency (CISA), *CISA Adds Three Known Exploited Vulnerabilities to Catalog*, CYBERSECURITY ADVISORY (May. 1, 2023), https://www.cisa.gov/news-events/alerts/2023/05/01/cisa-adds-three-known-exploited-vulnerabilities-catalog; National Institute of Standards and Technology, *National Vulnerability Database*, (Mar. 23, 2023), https://nvd.nist.gov/vuln/detail/CVE-2023-27078.

These vulnerabilities are especially problematic with routers and modems produced by entities with ties to foreign adversaries, particularly the Chinese Communist Party (CCP) in the People's Republic of China (PRC). The PRC "probably currently represents the broadest, most active, and persistent cyber espionage threat to U.S. Government and private-sector networks."[2] Indeed, the CCP could exploit several PRC laws to force China-based companies to share information companies collect on Americans or to sell unsecure equipment in the United States that the CCP could exploit for cyberattacks or espionage. For example, under the PRC's National Intelligence Law of 2017, the government can require individuals and entities to support its intelligence services, including by providing data without regard to where that data was collected and without any mechanism of due process.[3] Additionally, the 2021 Data Security Law expands the PRC's access to and control of companies and data within China and imposes strict penalties on China-based businesses for non-compliance. And the 2021 Cyber Vulnerability Reporting Law requires Chinese-based companies to disclose cyber vulnerabilities found in their systems or software to PRC authorities prior to any public disclosure or sharing overseas.[4] Given this, the CCP has the ability to exploit these laws by forcing router and modem manufacturers in China to turn over data that flows through the equipment they produce or sell vulnerable modem and router equipment to consumers in the United States.

COMMITTEE ACTION

On January 11, 2024, the Subcommittee on Communications and Technology held a hearing entitled, "Safeguarding Americans' Communications: Strengthening Cybersecurity in a Digital Era." The Subcommittee received testimony from:

- Jim Richberg, Head of Cyber Policy, Fortinet;
- Tobin Richardson, President and CEO, Connectivity Standards Alliance;
- Clete Johnson, Senior Fellow, Center for Strategic and International Studies; and
- Alan Butler, Executive Director and President, Electronic Privacy Information Center.

On February 15, 2024, the Subcommittee on Communications and Technology held a legislative hearing entitled, "Securing Communications Networks from Foreign Adversaries." The Subcommittee received testimony from:

- James Lewis, Senior Vice President, Center for Strategic and International Studies;
- Craig Singleton, China Program Senior Director and Senior Fellow, Foundation of Defense of Democracies; and

---

[2] U.S. Office of the Director of National Intelligence (ODNI), *Annual Threat Assessment of the U.S. Intelligence Community*, (Feb. 6, 2023), at 10, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf.

[3] U.S. Department of Homeland Security, Office of Strategy, Policy, and Plans Office of Trade and Economic Security, *Data Security Business Advisory: Risks and Considerations for Businesses Using Data Services and Equipment from Firms Linked to the People's Republic of China*, (Dec. 22, 2020), at 6, https://www.dhs.gov/sites/default/files/publications/20_1222_data-security-business-advisory.pdf.

[4] ODNI, National Counterintelligence and Security Center, *U.S. Business Risk: People's Republic of China (PRC) Laws Expand Beijing's Oversight of Foreign and Domestic Companies Safeguarding Our Future*, SAFEGUARDING OUR FUTURE BULLETIN (June 20, 2023), https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/FINAL_NCSC_SOF_Bulletin_PRC_Laws.pdf.

• Lindsay Gorman, Senior Fellow for Emerging Technologies, German Marshall Fund's Alliance for Securing Democracy.

On March 12, 2024, the Subcommittee on Communications and Technology met in open markup session and forwarded the ROUTERS Act (H.R. 7589 as introduced in the 118th Congress), without amendment, to the full Committee by a record vote of 23 yeas and 0 nays.

On March 20, 2024, the full Committee on Energy and Commerce met in open markup session and ordered H.R. 7589, without amendment, favorably reported to the House by a record vote of 43 yeas and 0 nays.

On April 8, 2025, the full Committee on Energy and Commerce met in open markup session and ordered H.R. 866, as amended, favorably reported to the House by a voice vote.

COMMITTEE VOTES

Clause 3(b) of rule XIII requires the Committee to list the record votes on the motion to report legislation and amendments thereto. There were no record votes taken in connection with ordering H.R. 866 reported.

OVERSIGHT FINDINGS AND RECOMMENDATIONS

Pursuant to clause 2(b)(1) of rule X and clause 3(c)(1) of rule XIII, the Committee held hearings and made findings that are reflected in this report.

NEW BUDGET AUTHORITY, ENTITLEMENT AUTHORITY, AND TAX EXPENDITURES

Pursuant to clause 3(c)(2) of rule XIII, the Committee finds that H.R. 866 would result in no new or increased budget authority, entitlement authority, or tax expenditures or revenues.

CONGRESSIONAL BUDGET OFFICE ESTIMATE

Pursuant to clause 3(c)(3) of rule XIII, at the time this report was filed, the cost estimate prepared by the Director of the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974 was not available.

FEDERAL MANDATES STATEMENT

The Committee adopts as its own the estimate of Federal mandates prepared by the Director of the Congressional Budget Office pursuant to section 423 of the Unfunded Mandates Reform Act.

STATEMENT OF GENERAL PERFORMANCE GOALS AND OBJECTIVES

Pursuant to clause 3(c)(4) of rule XIII, the general performance goal or objective of this legislation is to study the national security risks associated with routers, modems, and combined modem-router devices that are designed, developed, manufactured, or supplied by entities affiliated foreign adversaries.

DUPLICATION OF FEDERAL PROGRAMS

Pursuant to clause 3(c)(5) of rule XIII, no provision of H.R. 866 is known to be duplicative of another Federal program, including

any program that was included in a report to Congress pursuant to section 21 of Public Law 111–139 or the most recent Catalog of Federal Domestic Assistance.

RELATED COMMITTEE AND SUBCOMMITTEE HEARINGS

Pursuant to clause 3(c)(6) of rule XIII, the following hearings were used to develop or consider H.R. 866:

- On January 11, 2024, the Subcommittee on Communications and Technology held a hearing entitled, "Safeguarding Americans" Communications: Strengthening Cybersecurity in a Digital Era." The Subcommittee received testimony from:
  - Jim Richberg, Head of Cyber Policy, Fortinet;
  - Tobin Richardson, President and CEO, Connectivity Standards Alliance;
  - Clete Johnson, Senior Fellow, Center for Strategic and International Studies; and
  - Alan Butler, Executive Director and President, Electronic Privacy Information Center.
- On February 15, 2024, the Subcommittee on Communications and Technology held a legislative hearing entitled, "Securing Communications Networks from Foreign Adversaries." The Subcommittee received testimony from:
  - James Lewis, Senior Vice President, Center for Strategic and International Studies;
  - Craig Singleton, China Program Senior Director and Senior Fellow, Foundation of Defense of Democracies; and
  - Lindsay Gorman, Senior Fellow for Emerging Technologies, German Marshall Fund's Alliance for Securing Democracy.

COMMITTEE COST ESTIMATE

Pursuant to clause 3(d)(1) of rule XIII, the Committee adopts as its own the cost estimate prepared by the Director of the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974. At the time this report was filed, the estimate was not available.

EARMARK, LIMITED TAX BENEFITS, AND LIMITED TARIFF BENEFITS

Pursuant to clause 9(e), 9(f), and 9(g) of rule XXI, the Committee finds that H.R. 866 contains no earmarks, limited tax benefits, or limited tariff benefits.

ADVISORY COMMITTEE STATEMENT

No advisory committees within the meaning of Section 5(b) of the Federal Advisory Committee Act were created by this legislation.

APPLICABILITY TO LEGISLATIVE BRANCH

The Committee finds that the legislation does not relate to the terms and conditions of employment or access to public services or accommodations within the meaning of section 102(b)(3) of the Congressional Accountability Act.

SECTION-BY-SECTION ANALYSIS OF THE LEGISLATION

Section 1. Short title

This section would designate that the Act may be cited as the "Removing Our Unsecure Technologies to Ensure Reliability and Security Act" or the "ROUTERS Act."

Section 2. Study of national security risks posed by certain routers and modems

Subsection (a) would direct the Secretary of Commerce (Secretary) to conduct a study on the national security risks and cybersecurity vulnerabilities posed by consumer routers, modems, and combined modem-router devices that are designed, developed, manufactured, or supplied by entities affiliated with foreign adversaries, which are defined to mean the People's Republic of China, the Russian Federation, the Islamic Republic of Iran, and the Democratic People's Republic of North Korea.

Subsection (b) would direct the Secretary to submit a detailed report on the results of the study to the Committee on Energy and Commerce of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate within one year of enactment of the Act.

Subsection (c) would direct the Secretary to consult with appropriate bureaus and offices within the Department of Commerce in conducting this study.

Subsection (d) would define terms used in this section, including that the term "Secretary" means the Secretary of Commerce acting through the Assistant Secretary of Commerce for Communications and Information.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

This legislation does not amend any existing Federal statute.