

UNDERSTANDING CYBERSECURITY OF MOBILE
NETWORKS ACT

JUNE 30, 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. 1709]

[Including cost estimate of the Congressional Budget Office]

The Committee on Energy and Commerce, to whom was referred
the bill (H.R. 1709) to direct the Assistant Secretary of Commerce
for Communications and Information to submit to Congress a re-
port examining the cybersecurity of mobile service networks, and
for other purposes, having considered the same, reports favorably
thereon without amendment and recommends that the bill do pass.

CONTENTS

	Page
Purpose and Summary	2
Background and Need for Legislation	2
Committee Action	2
Committee Votes	3
Oversight Findings and Recommendations	3
New Budget Authority, Entitlement Authority, and Tax Expenditures	3
Congressional Budget Office Estimate	3
Federal Mandates Statement	4
Statement of General Performance Goals and Objectives	4
Duplication of Federal Programs	4
Related Committee and Subcommittee Hearings	4
Committee Cost Estimate	4
Earmark, Limited Tax Benefits, and Limited Tariff Benefits	4
Advisory Committee Statement	4
Applicability to Legislative Branch	5
Section-by-Section Analysis of the Legislation	5
Changes in Existing Law Made by the Bill, as Reported	5

PURPOSE AND SUMMARY

H.R. 1709, the “Understanding Cybersecurity of Mobile Networks Act,” was introduced by Representative Greg Landsman (D–OH) on February 27, 2025. It would direct the Assistant Secretary of Commerce for Communications and Information to submit to Congress a report examining the cybersecurity of mobile service networks.

BACKGROUND AND NEED FOR LEGISLATION

Federal agencies, academic researchers, and independent experts have examined various and disparate aspects of, specific threats to, and vulnerabilities of the cybersecurity of mobile devices and networks.¹ Providers of mobile services, along with manufacturers of mobile devices and other companies, have responded to many vulnerabilities and threats.² However, recent cybersecurity developments show that vulnerabilities continue to exist in mobile cybersecurity, including threats of mobile data interception by cell site simulators,³ identity theft via fraudulent SIM swaps,⁴ and surveillance enabled by spyware installed on mobile devices.⁵ Policy-makers lack a holistic accounting of what vulnerabilities have been addressed or are being addressed and which ones persist.

While policymakers and industry actors are appropriately focused on cybersecurity of 5G networks, cybersecurity related to 2G, 3G, and 4G networks is of particular public policy interest because these networks host a vast majority of Americans’ mobile calls and text messages and mobile internet data traffic.

While many Federal agencies have authorities and responsibilities related to cybersecurity, Congress has tasked NTIA to foster safety and national security of telecommunications networks.⁶

COMMITTEE ACTION

The Committee on Energy and Commerce held a hearing in the development of the legislation during the 119th Congress. On January 23, 2025, the Subcommittee on Communications and Technology held a hearing. The title of the hearing was “Strengthening American Leadership in Wireless Technology.” The Subcommittee received testimony from the following witnesses:

- Michael K. Powell, President & CEO, NCTA—The Internet & Television Association;
- Brad Gillen, Executive Vice President, CTIA—The Wireless Association;
- Diane Rinaldo, Executive Director, Open RAN Policy Coalition; and
- Chris Lewis, President & CEO, Public Knowledge.

On March 4, 2025, the full Committee on Energy and Commerce met in open markup session and ordered H.R. 1709 favorably reported to the House by a voice vote.

¹See, e.g., Department of Homeland Security, *Study on Mobile Device Security* (April 2017).

²See, e.g., CTIA, *SS7 and FCC CSRIC Recommendations* (2017).

³Lily Hay Newman, *One Small Fix Would Curb Stingray Surveillance*, *Wired* (January 27, 2020).

⁴M.J. Kelly, *Mozilla Explains: SIM swapping*, *Mozilla* (April 7, 2021).

⁵Mitchell Clark, *NSO’s Pegasus spyware: here’s what we know*, *The Verge* (July 23, 2021).

⁶National Telecommunications and Information Administration Organization Act § 102(c)(2), 47 U.S.C. § 901(c)(2).

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. 1709 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. 1709 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, the following is the cost estimate provided by the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974:

H.R. 1709, Understanding Cybersecurity of Mobile Networks Act			
As ordered reported by the House Committee on Energy and Commerce on March 4, 2025			
By Fiscal Year, Millions of Dollars	2025	2025-2030	2025-2035
Direct Spending (Outlays)	0	0	0
Revenues	0	0	0
Increase or Decrease (-) in the Deficit	0	0	0
Spending Subject to Appropriation (Outlays)	*	*	not estimated
Increases <i>net direct spending</i> in any of the four consecutive 10-year periods beginning in 2036?	No	Statutory pay-as-you-go procedures apply? No	
Increases <i>on-budget deficits</i> in any of the four consecutive 10-year periods beginning in 2036?	No	Mandate Effects	
		Contains intergovernmental mandate?	No
		Contains private-sector mandate?	No
* = between zero and \$500,000.			

H.R. 1709 would require the Department of Commerce to assess the effectiveness of cybersecurity practices employed by providers of mobile communications services and to report to the Congress on cybersecurity vulnerabilities of mobile networks and devices.

Using information about the cost of similar requirements, CBO estimates that implementing the bill would cost less than \$500,000. Such spending would be subject to the availability of appropriated funds.

The CBO staff contact for this estimate is Aldo Prosperi. The estimate was reviewed by Christina Hawley Anthony, Deputy Director of Budget Analysis.

PHILLIP L. SWAGEL,
Director, Congressional Budget Office.

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 require the Assistant Secretary of Commerce for Communications and Information, in consultation with the Department of Homeland Security, to encourage participation by trusted companies and other stakeholders in various standards-setting bodies.

DUPLICATION OF FEDERAL PROGRAMS

Pursuant to clause 3(c)(5) of rule XIII, no provision of H.R. 1709 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 related hearing was used to develop or consider H.R. 1709:

On January 23, 2025, the Subcommittee on Communications and Technology held a hearing. The title of the hearing was “Strengthening American Leadership in Wireless Technology.” The Subcommittee received testimony from the following witnesses:

- Michael K. Powell, President & CEO, NCTA—The Internet & Television Association;
- Brad Gillen, Executive Vice President, CTIA—The Wireless Association;
- Diane Rinaldo, Executive Director, Open RAN Policy Coalition; and
- Chris Lewis, President & CEO, Public Knowledge.

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.

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. 1709 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 designates that the short title may be cited as the “Understanding Cybersecurity of Mobile Networks Act.”

Sec. 2. Report on cybersecurity of mobile service networks

Subsection (a) directs the Assistant Secretary of Commerce for Communications and Information (i.e. the Administrator of the National Telecommunications and Information Administration), in consultation with the Department of Homeland Security, to submit to Congress, not later than one year after enactment, a report examining the cybersecurity of mobile service networks and the vulnerability of such networks and mobile devices to cyberattacks and surveillance conducted by adversaries.

Subsection (b) requires the report to include (1) an assessment of the degree to which providers of mobile service have addressed cybersecurity vulnerabilities; (2) a discussion of the degree to which customers consider cybersecurity; (3) a discussion of best practices and risk assessment frameworks; (4) an estimate and discussion of aspects of encryption and authentication algorithms and techniques; (5) a discussion of barriers to more efficacious encryption; (6) an estimate and discussion of aspects of authentication; and (7) an estimate and discussion of aspects of cell site simulators and other surveillance technologies.

Subsection (c) requires the Assistant Secretary, in preparing the report, to consult certain Federal agencies; researchers; participants in multistakeholder standards organizations; international stakeholders; industry representatives; and other experts.

Subsection (d) provides certain limitations on the scope of the report, including that the report shall exclude consideration of 5G and limit vulnerabilities to those that have been exploited or are feasibly exploitable.

Subsection (e) provides that the report shall be produced in an unclassified form, shall redact potentially exploitable unclassified information, and may contain a classified annex.

Subsection (f) provides definitions for certain terms used in the Act, including adversary, mobile communications equipment or service, and mobile service.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

This legislation does not amend any existing Federal statute.