Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Protecting the Nation's Communications Systems from Cybersecurity Threats	)	PS Docket No. 22-329
	)	

ORDER ON RECONSIDERATION

Adopted: November 20, 2025 **Released: November 21, 2025**

By the Commission: Chairman Carr and Commissioner Trusty issuing separate statements; Commissioner Gomez dissenting and issuing a separate statement.

TABLE OF CONTENTS

I. INTRODUCTION

1. Foreign adversaries and other bad actors are consistently attempting to jeopardize America's national security by launching cyberattacks against our communications networks. That is why this FCC has bolstered the agency's work to address these threats through numerous rulemakings and enforcement actions.[1] As part of its efforts to do so, the FCC stood up a new Council on National

[1] *See*, *e.g.*, *Review of Submarine Cable Landing License Rules and Procedures to Assess Evolving National Security, Law Enforcement, Foreign Policy, and Trade Policy Risks*; *Amendment of the Schedule of Application Fees Set Forth in Sections 1.1102 through 1.1109 of the Commission's Rules*, OI Docket No. 24-523, MD Docket No. 24-524, Report and Order and Further Notice of Proposed Rulemaking, FCC 25-49 (Aug. 13, 2025) (*Submarine Cable Order/FNPRM*); *Promoting the Integrity and Security of Telecommunications Certification Bodies, Measurement Facilities, and the Equipment Authorization Program*, ET Docket No. 24-136, Report and Order and Further Notice of Proposed Rulemaking, FCC 25-27 (May 27, 2025); *see also* Press Release, FCC, FCC Takes Action on "Bad Labs" Apparently Controlled By China (Sept. 8, 2025), https://docs.fcc.gov/public/attachments/DOC-414369A1.pdf; Press Release, FCC Denies Second Batch of "Bad Labs" Controlled By China (Sept. 26, 2025), https://docs.fcc.gov/public/attachments/DOC-414863A1.pdf; Press Release, FCC, Carr Announces Sweeping New (continued….)

Security within the agency earlier this year,[2] and we have been working with network providers since the beginning of the year.

2. Following these FCC engagements with carriers, providers agreed this year to take "extensive, urgent, and coordinated efforts to mitigate operational risks, protect consumers, and preserve national security interests" against the range of cyberattacks that target their networks.[3] In particular, through a collaborative approach, providers have agreed to implement additional cybersecurity controls to harden their networks.[4] These controls have included accelerated patching of outdated or vulnerable equipment, updating and reviewing access controls, disabling unnecessary outbound connections, and improving their threat-hunting efforts.[5] Providers have also committed to increased cybersecurity information sharing, both with the federal government and within the communications sector.[6] This represents a significant change in cybersecurity practices compared to the measures in place in January.

3. In light of these changes, the Commission takes two actions today. First, we reconsider and rescind a January 16, 2025, Declaratory Ruling issued by the prior FCC.[7] As explained below, that decision was both an unlawful and ineffective attempt to show that the agency was taking some type of action on cybersecurity issues. It was unlawful because the FCC purported to read a statute that required telecommunications carriers to allow lawful wiretaps within a certain portion of their network as a provision that required carriers to adopt specific network management practices in every portion of their network. It was ineffective because it neither responded to the nature of the relevant cybersecurity threats nor was it consistent with the agile and collaborative approach to cybersecurity that has proven successful.

4. Second, and for similar reasons, we are withdrawing the Notice of Proposed Rulemaking (NPRM) that accompanied the Declaratory Ruling.[8] The FCC must focus its resources on advancing cybersecurity protections that are both lawful and effective. Collaboration with carriers, coupled with targeted, legally robust regulatory and enforcement measures, has proven successful—more so than the proposed one-size-fits-all approach announced in the Declaratory Ruling and proposed in the NPRM.

II. BACKGROUND

5. U.S. communications networks are vulnerable to cyber exploits that pose significant risks to national security, public safety, and economic stability. The increasing sophistication of cyberattacks,

(Continued from previous page)
Investigation into CCP-Aligned Entities (Mar. 21, 2025), https://docs.fcc.gov/public/attachments/DOC-410318A1.pdf; *HKT (International) Limited et al.*, GN Docket No. 25-308, Order to Show Cause, DA-25-928 (OIA Oct. 15, 2025); Press Release, FCC, FCC Approves New Safeguards Against Untrustworthy Gear (Oct. 28, 2025), https://docs.fcc.gov/public/attachments/DOC-415131A1.pdf.

[2] Press Release, FCC, Chairman Carr Establishes New Council on National Security Within Agency (Mar. 13, 2025), https://docs.fcc.gov/public/attachments/DOC-410155A1.pdf.

[3] Letter from Thomas M. Johnson, Jr., and Megan L. Brown, Wiley Rein LLP, to Marlene H. Dortch, FCC, EB Docket No. 22-329 (filed Oct. 16, 2025) (Oct. 16, 2025 CTIA *Ex Parte*).

[4] *Id*. at 9.

[5] *Id*. at 9-10.

[6] *Id*.

[7] *Protecting the Nation's Communications Systems from Cybersecurity Threats*, PS Docket No. 22-329, Declaratory Ruling and Notice of Proposed Rulemaking, FCC 25-9, 40 FCC Rcd 876 (2025) (*Declaratory Ruling* or *NPRM*, as appropriate); Petition for Reconsideration of CTIA – The Wireless Association, NCTA – The Internet & Television Association, and USTelecom – The Broadband Association, PS Docket No. 22-329 (filed Feb. 18, 2025), https://www.fcc.gov/ecfs/document/102183024015116/1 (Petition).

[8] *See NPRM*, 40 FCC Rcd at 885-921, paras. 16-72 & Appendix A (Proposed Rules).

particularly those linked to the People's Republic of China (PRC), highlights the urgent need for cybersecurity measures. For example, in September 2024, it was disclosed that the PRC-sponsored advanced persistent threat group Salt Typhoon had infiltrated at least eight U.S. communications companies as part of a massive espionage campaign that affected dozens of countries.[9] The attacks exploited publicly known common vulnerabilities and exposures (CVEs) and other avoidable weaknesses to compromise networks, rather than zero-day (i.e., previously undisclosed) vulnerabilities.[10] These attacks "reflect[] a pattern of targeting the [communications] sector for both its role in enabling other sectors, and also the value of the systems and data contained within the sector itself."[11]

6. Congress created the Commission, among other reasons, "for the purpose of the national defense . . . ."[12] The Commission's commitment to improving the security of the nation's communications networks remains steadfast, as demonstrated by coordinated efforts and rulemakings to protect the security of our nation's communications networks and infrastructure from potential security threats.

A. Recent Commission Action to Protect the Nation's Communications Systems

7. The Commission has taken a series of recent actions to harden communications networks and improve their security posture. The Commission works closely with federal partner agencies and carriers to identify vulnerabilities, risks, and threats, and convey real-time guidance to protect networks from foreign adversaries, like the PRC.[13] In March 2025, the Commission established a Council on National Security within the Commission to, among other things, "facilitate the Commission's engagement with national security partners across the Executive Branch and in Congress"[14] and "mitigate America's vulnerabilities to cyberattacks, espionage, and surveillance by foreign adversaries."[15] The Commission also investigates communications network outages that result from cyber incidents, and its Public Safety and Homeland Security Bureau recently published a Public Notice seeking comment from

[9] Sarah Krouse et al., *China-Linked Hackers Breach U.S. Internet Providers in New 'Salt Typhoon' Cyberattack*, Wall Street Journal (Sept. 26, 2024), https://www.wsj.com/politics/national-security/china-cyberattack-internet-providers-260bd835; Chris Jaikaran, *Salt Typhoon Hacks of Telecommunications Companies and Federal Response Implications*, Congress.gov (Jan. 23, 2025), https://www.congress.gov/crs-product/IF12798 (CRS Salt Typhoon Report).

[10] National Security Agency et al., Joint Cybersecurity Advisory, *Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System* (Sept. 3, 2025), https://media.defense.gov/2025/Aug/22/2003786665/-1/-1/0/CSA_COUNTERING_CHINA_STATE_ACTORS_COMPROMISE_OF_NETWORKS.PDF.

[11] Chris Jaikaran, *Salt Typhoon Hacks of Telecommunications Companies and Federal Response Implications*, Congress.gov (Jan. 23, 2025), https://www.congress.gov/crs-product/IF12798 (CRS Salt Typhoon Report).

[12] Communications Act of 1934, Pub. L. No. 73-416, § 1, 48 Stat. 1064, 1064 (1934); *see also* 47 U.S.C. § 151 (amended to read "for the purpose of the national defense [and] for the purpose of promoting safety of life and property through the use of wire and radio communications").

[13] *See* Office of the Director of National Intelligence, Annual Threat Assessment of the U.S. Intelligence Community, at 9-16 (2025), https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf.

[14] Press Release, FCC, Chairman Carr Establishes New Council on National Security Within Agency (Mar. 13, 2025), https://docs.fcc.gov/public/attachments/DOC-410155A1.pdf.

[15] *See* FCC Council on National Security, https://www.fcc.gov/fcc-council-national-security.

the public and the public safety community about a recent outage that reportedly resulted from a ransomware attack.[16]

8. The Commission has also adopted targeted rules to address the greatest cybersecurity risks to critical communications infrastructure without imposing inflexible and ambiguous requirements. For instance, the Commission recently adopted a Report and Order, based on a record developed through notice-and-comment rulemaking, that requires licensees that operate submarine cable networks to create and implement cybersecurity risk management plans.[17] That action included a Further Notice of Proposed Rulemaking that proposes to fast-track submarine cable applications by presumptively exempting them from Executive Branch review if they meet certain enhanced physical and cybersecurity standards, among other requirements.[18]

9. In May 2025, the Commission also adopted a Report and Order and Further Notice of Proposed Rulemaking adopting rules to ensure that test labs, telecommunications certification bodies, and laboratory accreditation bodies recognized in the FCC's equipment authorization program are not subject to ownership, direction, or control by untrustworthy actors that pose a risk to national security, including China. In September, we announced that we have begun proceedings to withdraw recognition from these "bad labs."[19] We are investigating the continued U.S. operations of Chinese Communist Party (CCP)-aligned businesses whose equipment or services the Commission placed on its Covered List.[20] In October, we began the process to revoke HKT (International) Limited's domestic authority and revoke and terminate its international authority pursuant to section 214 of the Communications Act of 1934, and addressed security vulnerabilities in electronic equipment marketed in the United States by closing two potential loopholes in our equipment authorization program and proposing to extend our equipment security rules to a larger class of foreign adversary-controlled devices.[21]

B. Other Communications Sector Cybersecurity Measures

10. Many communications service providers are already subject to existing or forthcoming federal cybersecurity requirements. For example, the Securities and Exchange Commission (SEC) requires public companies to describe their processes for assessing, identifying, and managing material risks from cybersecurity threats, as well as board of directors and management oversight of those risks,[22] as part of registration statements, annual reports, and other filings.[23] Public companies must also disclose

[16] *See Public Safety and Homeland Security Bureau Seeks Information on Effects of May 2025 Cellcom Outage on Consumers, Public Safety Entities, and Government Entities*, Public Notice, DA 25-607 (PSHSB 2025), https://docs.fcc.gov/public/attachments/DA-25-607A1.pdf.

[17] *Submarine Cable Order/FNPRM*.

[18] *See Submarine Cable Order/FNPRM* at 128-36, paras. 283-301.

[19] *Promoting the Integrity and Security of Telecommunications Certification Bodies, Measurement Facilities, and the Equipment Authorization Program*, ET Docket No. 24-136, Report and Order and Further Notice of Proposed Rulemaking, FCC 25-27 (May 27, 2025). *See* Press Release, FCC, FCC Takes Action on "Bad Labs" Apparently Controlled By China (Sept. 8, 2025), https://docs.fcc.gov/public/attachments/DOC-414369A1.pdf; Press Release, FCC Denies Second Batch of "Bad Labs" Controlled By China (Sept. 26, 2025), https://docs.fcc.gov/public/attachments/DOC-414863A1.pdf.

[20] Press Release, FCC, Carr Announces Sweeping New Investigation into CCP-Aligned Entities (Mar. 21, 2025), https://docs.fcc.gov/public/attachments/DOC-410318A1.pdf.

[21] *HKT (International) Limited et al.*, GN Docket No. 25-308, Order to Show Cause, DA-25-928 (OIA Oct. 15, 2025); Press Release, FCC, FCC Approves New Safeguards Against Untrustworthy Gear (Oct. 28, 2025), https://docs.fcc.gov/public/attachments/DOC-415131A1.pdf.

[22] 17 CFR § 229.106(b)-(c).

[23] 17 CFR § 229.10(a).

any material cybersecurity incident and describe material aspects of the nature, scope, and timing of the incident, as well as the impact of the incident, in Form 8-K filings.[24] Additionally, many carriers are subject to state laws that require them to implement reasonable cybersecurity risk management practices to protect customer data.[25] The Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), as amended, also requires the Cybersecurity and Infrastructure Security Agency (CISA) to promulgate regulations implementing CIRCIA's covered cyber incident and ransom payment reporting requirements for covered entities,[26] including those in critical infrastructure sectors like communications.[27] CISA sought comment on cyber incident reporting requirements in June 2024[28] and has indicated it expects to adopt a final rule in May 2026.[29]

11. Moreover, some providers voluntarily adhere to industry and government cybersecurity standards. For example, the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0 provides guidance to industry, government agencies, and other organizations to help manage cybersecurity risks.[30] The CSF "describes what desirable outcomes an organization can aspire to" but "does not prescribe outcomes nor how they can be achieved," instead suggesting the CSF should be used in conjunction with other resources like frameworks, standards, and guidelines.[31] Many wireless carriers, including AT&T, Verizon, and T-Mobile, assert that they follow practices that align with the CSF or incorporate its core functions into their cybersecurity programs.[32] CISA also provides voluntary tools and services to aid in strengthening cybersecurity practices,[33] including the Cybersecurity Performance Goals (CPGs), which are baseline practices that critical infrastructure entities can use to manage and reduce cybersecurity risks.[34] CISA's cross-sector CPGs provide sector-agnostic, prioritized guidance to help organizations focus resources on the most effective risk-reduction measures.[35] To

[24] *See* 17 CFR § 249.308; SEC, Form 8K: Instructions at 11-12, https://www.sec.gov/files/form8-k.pdf (last visited Oct. 24, 2025) (describing procedure for reporting material cybersecurity incidents).

[25] *See, e.g.,* Cal. Civ. Code § 1798.100(e); N.Y. Gen. Bus. Law § 899-bb(2); Tex. Bus. & Com. Code § 541.101(a)(2); Va. Code § 59.1-578(A)(3). *See also* Complaint, *Washington v. T-Mobile US*, No. 25-2-00308-6 SEA, at 22-25 (Wash. Super. Ct. Jan 6, 2025) (alleging that T-Mobile violated Washington's Consumer Protection Act, RCW 19.86.020, by "failing to implement adequate cybersecurity risk management . . . [and] network configuration management").

[26] 6 U.S.C. § 681b(a)(1)-(3), (b).

[27] 6 U.S.C. § 681.

[28] *See* CISA, *Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements NPRM*, 89 FR 23644 (Apr. 4, 2024).

[29] *See* OIRA, *Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements*, https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202504&RIN=1670-AA04 (last visited Sept. 19, 2025) (showing a "final rule" date of "05/00/2026").

[30] NIST, NIST Cybersecurity Framework (CSF) 2.0 (2024), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf (NIST CSF 2.0).

[31] NIST CSF 2.0 at 6-7.

[32] CTIA Comments, Docket No. 220210-0045, at 4 (Apr. 25, 2022), https://www.nist.gov/system/files/documents/2022/05/03/04-25-2022%20-%20CTIA.pdf.

[33] *See, e.g.,* CISA, *CISA Vulnerability Scanning*, https://www.cisa.gov/resources-tools/services/cisa-vulnerability-scanning (last visited Sept. 15, 2025) (offering vulnerability scanning at no cost for critical infrastructure, including communications providers).

[34] CISA, *Cybersecurity Performance Goals*, https://www.cisa.gov/cybersecurity-performance-goals-cpgs (last visited Sept. 18, 2025).

[35] *Id.*

support CPG adoption, CISA offers Assessment Training with regional cybersecurity experts to help communications providers better understand the CPGs and cybersecurity risk assessment.[36] The Telecommunications Industry Association (TIA) also sells a standard providing baseline security requirements that apply to all aspects of the information and communications technology supply chain, including "processes for identifying, addressing, and reporting security risks to minimize the potential for attack and adverse impact on consumers and businesses."[37]

C. The Communications Assistance for Law Enforcement Act (CALEA)

12. Congress enacted CALEA in 1994 "to preserve the ability of law enforcement officials to conduct authorized electronic surveillance in the face of the recent, rapid technological changes in telecommunications that threaten their ability to intercept communications."[38] As the Commission recognized in its first Notice of Proposed Rulemaking on its implementation of CALEA, "CALEA assigns certain responsibilities to the Commission and permits it, at its discretion, to assume others."[39] Among those responsibilities is the duty to adopt rules to implement the "systems security and integrity" obligations of section 105 of CALEA.[40] The Commission has implemented these responsibilities in multiple rulemaking proceedings for nearly thirty years, including specific rules implementing both section 105 and the assistance-capability requirements of section 103.[41] The Commission has also cited these duties in adopting other rules directed at preventing carriers from allowing unauthorized surveillance within their networks.[42]

13. Other Commission proceedings implementing CALEA have interpreted or applied section 103 of that statute, which requires telecommunications carriers to ensure that their equipment, services, and facilities meet four "assistance capability" requirements.[43] Those requirements are directed at ensuring that carriers' networks are capable of assisting the government in conducting lawfully authorized electronic surveillance, including by intercepting a subscriber's communications; providing

---

[36] CISA, *Cybersecurity Performance Goals (CPG) Assessment Training,* https://www.cisa.gov/resources-tools/training/cybersecurity-performance-goals-cpg-assessment-training (last visited Sept. 15, 2025).

[37] *See* Telecommunications Industry Association, *SCS 9001 Cyber and Supply Chain Security Standard*, https://tiaonline.org/what-we-do/scs-9001-supply-chain-security-standard/ (last visited Oct. 8, 2025).

[38] *Communications Assistance for Law Enforcement Act*, CC Docket No. 97-213, Notice of Proposed Rulemaking, 13 FCC Rcd 3149, 3154, para. 5 (*1997 CALEA NPRM*) (citing 140 Cong. Rec. H-10779 (daily ed. Oct. 7, 1994) (statement of Rep. Hyde)); *see* Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified at 47 U.S.C. §§ 229, 1001-1010) (CALEA).

[39] *1997 CALEA NPRM*, 13 FCC Rcd at 3156, para. 9 (citing 47 U.S.C. § 229(a)).

[40] *See* 47 U.S.C. § 229(b); *see also* CALEA § 105, 47 U.S.C. § 1004 ("A telecommunications carrier shall ensure that any interception of communications or access to call-identifying information effected within its switching premises can be activated only in accordance with a court order or other lawful authorization and with the affirmative intervention of an individual officer or employee of the carrier acting in accordance with regulations prescribed by the Commission.").

[41] 47 CFR §§ 1.20000-1.20008. *See, e.g.*, *1997 CALEA NPRM*; *Communications Assistance for Law Enforcement Act*, Report and Order, 14 FCC Rcd 4151, 4151, para. 1 (1999) ("establish[ing] the systems security and integrity regulations that telecommunications carriers must follow to comply with section 105 of CALEA"); *Communications Assistance for Law Enforcement Act and Broadband Access and Services*, Notice of Proposed Rulemaking and Declaratory Ruling, ET Docket No. 04-295, RM-10865, 19 FCC Rcd 15676, 15678-91, paras. 5-29 (2004) (discussing the 1994-2004 history of the Commission's CALEA implementation actions and orders).

[42] *See, e.g.*, *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, Report and Order, Further Notice of Proposed Rulemaking, and Order, 34 FCC Rcd 11423, 11436-37, paras. 35-37 (2019) (*Supply Chain First Report and Order*).

[43] 47 U.S.C. § 1002(a)(1)-(4).

access to call-identifying information that is reasonably available to the carrier; delivering such communications and information to the government; and doing so unobtrusively in a way that protects the privacy and security of communications and information not authorized to be intercepted and information regarding the government's authorized surveillance activities. Section 103 expressly "does not authorize any law enforcement agency or officer" to either require that carriers adopt, or prohibit carriers from adopting, "any specific design of equipment, facilities, services, features, or system configurations."[44] Section 107 provides that a carrier shall be found to be in compliance with section 103 if it complies with "publicly available technical requirements or standards adopted by an industry association or standard-setting organization," or by the Commission in response to a petition from the government or from any person who believes such technical requirements or standards are deficient.[45]

14. The scope of CALEA's applicability is notably affected by its definition of "telecommunications carrier," which includes an entity providing a service that the Commission finds to be "a replacement for the substantial portion of the local telephone exchange service" if doing so is in the public interest.[46] Based on this "Substantial Replacement Provision," in 2005, the Commission interpreted CALEA's definition of "telecommunications carrier" as "broader than that found in the Communications Act"[47] and as including facilities-based broadband Internet access service (BIAS) providers and interconnected Voice over Internet Protocol (VoIP) service providers.[48]

D. January 2025 Declaratory Ruling and Notice of Proposed Rulemaking

15. On January 15, 2025, five days before the change in administration, the Commission adopted the Declaratory Ruling and NPRM without prior public notice or any opportunity for public comment. The Declaratory Ruling "conclud[ed] that section 105 of CALEA affirmatively requires telecommunications carriers . . . to secure their networks from unlawful access to or interception of communications."[49] It interpreted section 105 by purporting to "clarify that telecommunications carriers' duties under section 105 of CALEA extend not only to the equipment they choose to use in their networks, but also to how they manage their networks."[50] It reasoned that, because section 105 requires that carriers "'shall ensure' that the 'only' interception of communications or access to call-identifying information is that which is" authorized, "CALEA obligates carriers to *prevent* interception of communications or access to call-identifying information by any other means."[51] From this, the Declaratory Ruling concluded that "section 105 of CALEA independently obligates telecommunications carriers to prevent all incidents of unauthorized interception of communications and access to call-identifying information, not merely those carried out by law enforcement."[52]

16. Based on this interpretation, the Declaratory Ruling stated that carriers would be "unlikely" to satisfy these statutory obligations "without adopting certain basic cybersecurity practices for

---

[44] 47 U.S.C. § 1002(b)(1).

[45] 47 U.S.C. § 1006(a), (b).

[46] 47 U.S.C. § 1001(8)(B)(ii).

[47] *Communications Assistance for Law Enforcement Act and Broadband Access and Services*, ET Docket No. 04-295, RM-10865, First Report and Order and Further Notice of Proposed Rulemaking, 20 FCC Rcd 14989, 14993, para. 10 (2005), *aff'd*, *American Council on Educ. v. FCC*, 451 F.3d 226 (D.C. Cir. 2006).

[48] *Id.* at 14989, 14991-92, 15002-12, paras. 8, 26-45.

[49] *Declaratory Ruling*, 40 FCC Rcd at 883, para. 11.

[50] *Id.* (footnote omitted).

[51] *Id.* at 884, para. 12.

[52] *Id.* at 884, para. 13.

their communications systems and services," such as "implementing role-based access controls, changing default passwords, requiring minimum password strength, and adopting multifactor authentication."[53] It further stated that "a failure to patch known vulnerabilities or to employ best practices that are known to be necessary in response to identified exploits would appear to fall short of fulfilling this statutory obligation."[54] It described as "necessary" that the following practices be implemented at the enterprise level:

> Enterprise-level implementation of these basic cybersecurity hygiene practices is necessary to prevent unlawful real-time access to communications because vulnerabilities in ancillary systems, operational networks, or administrative infrastructure can provide attackers with unauthorized access that can ultimately compromise surveillance systems and other network elements. For example, even well-protected switches within an otherwise unsecured network would be vulnerable to compromise through the integration of infected systems in the supply chain or lateral movement by threat actors within the network. The integration of cybersecurity best practices across an enterprise makes it less likely that attackers can gain unauthorized access to networks from more common points of entry, such as corporate IT systems, customer-facing portals, and third-party vendors.[55]

17. Also based on this interpretation of CALEA section 105, the Declaratory Ruling concluded that Congress had authorized the Commission to adopt rules that require telecommunications carriers (as defined for purposes of CALEA) to take specific steps to secure their networks against unauthorized interception.[56] The Declaratory Ruling was effective immediately.[57]

18. The NPRM proposed cybersecurity rules that would apply to a broad range of "Covered Providers," which it defined as including facilities-based BIAS providers; all broadcasting stations; all cable systems; wireline video systems; wireline communications providers; commercial radio operators; interconnected VoIP providers; telecommunications relay service providers; satellite communications providers; commercial mobile radio providers; wireless resellers and Mobile Virtual Network Operators; covered 911 service providers; covered 988 service providers; and international section 214 authorization holders.[58] The proposed rules would require those entities to create, update, and implement cybersecurity and supply chain risk management plans, and also to take reasonable measures to protect the confidentiality, integrity, and availability of their systems and services that could affect their provision of communications service.[59] The Commission described various sources of legal authority that it believed would, together, provide a basis for applying those requirements to each of the types of Covered

[53] *Id.* at 884-85, para. 14.

[54] *Id.* at 885, para. 14.

[55] *Id.* at 885, para. 14.

[56] *Id.* at 885, para. 15.

[57] *See NPRM*, 40 FCC Rcd at 885, para. 16 ("The Declaratory Ruling above establishes that telecommunications carriers subject to CALEA have a statutory obligation and is effective immediately."); *id.* at 9116, para. 91 (ordering clause adopting the *Declaratory Ruling and Notice of Proposed Rulemaking*); 47 CFR § 1.103(a) (providing that "the Commission may . . . designate an effective date that is either earlier or later in time than the date of public notice of such action.").

[58] *NPRM*, 40 FCC Rcd at 886-88, para. 16; *id.* at 917-18, Appendix A § 12.1 (Proposed Rules).

[59] *Id.* at 890, para. 18; *id.* at 918-19, Appendix A § 12.2 (Proposed Rules).

Providers.[60] For statutory authority to impose the proposed requirements on telecommunications carriers as defined by CALEA, it relied in part on the conclusion of the Declaratory Ruling.[61]

19. On February 18, 2025, CTIA – The Wireless Association, NCTA – The Internet & Television Association, and USTelecom – The Broadband Association (Petitioners) filed a Petition for Reconsideration asking the Commission to rescind the Declaratory Ruling.[62] On February 28, 2025, the Electronic Privacy Information Center (EPIC) filed an Opposition to the Petition.[63] Petitioners submitted a reply on March 10, 2025.[64] Petitioners, EPIC, and the Texas Association of Business subsequently submitted *ex parte* filings.[65]

20. In a further October 16, 2025 *ex parte* letter, Petitioners identified ways in which the communications sector has worked with the federal government and made further commitments to harden their networks. With respect to coordination with the federal government and across the sector, the Petitioners highlighted the communications sector's participation in the National Coordinating Center for Telecommunications' Communications Information Sharing and Analysis Center (Comm-ISAC), and noted that some providers have participated in the Commission's Communications Security, Reliability, and Interoperability Council (CSRIC), which has prepared a series of reports concerning cybersecurity risks affecting the communications sector and identifying best practices to mitigate those risks.[66] According to Petitioners, these forums and other collaborative activities involving CISA, federal law

[60] *See id.* at 899-909, paras. 35-54.

[61] *See id.* at 902-03, paras. 43-44.

[62] Petition for Reconsideration of CTIA – The Wireless Association, NCTA – The Internet & Television Association, and USTelecom – The Broadband Association, PS Docket No. 22-329 (filed Feb. 18, 2025), https://www.fcc.gov/ecfs/document/102183024015116/1 (Petition). Petitioners filed their Petition before publication of the Declaratory Ruling in the Federal Register. The Petition may therefore have been premature, *see* 47 CFR § 1.4(b)(1), but we need not resolve that issue because we may consider the merits of the petition on our own motion, 47 CFR § 1.108. *See, e.g.*, *Review of the Emergency Alert System, et al.*, Order on Reconsideration, 27 FCC Rcd 4429, 4431-32, para. 6 & n.16 (2012) ("[B]efore publication of the *Fifth Report and Order* in the Federal Register on March 22, 2012, a number of filings requesting similar action were made in this docket. We do not treat these requests as petitions for reconsideration that are properly filed, but rather consider their merits on our own motion." (citation omitted)).

[63] Electronic Privacy Information Center (EPIC) Opposition to Petition for Reconsideration of CTIA – The Wireless Association, NCTA – The Internet & Television Association, and USTelecom – The Broadband Association, PS Docket No. 22-329 (filed Feb. 28, 2025), https://www.fcc.gov/ecfs/document/1022867314705/1 (Opposition).

[64] Reply in Support of Petition for Reconsideration of CTIA – The Wireless Association, NCTA – The Internet & Television Association, and USTelecom – The Broadband Association, PS Docket No. 22-329 (filed Mar. 10, 2025), https://www.fcc.gov/ecfs/document/10307235647513/1 (Reply).

[65] *See* Letter from Thomas M. Johnson, Jr., and Megan L. Brown, Wiley Rein LLP, to Marlene H. Dortch, FCC, EB Docket No. 22-329 (filed July 25, 2025); Letter from Chris Frascella and Michelle Ly, EPIC, to Marlene Dortch, FCC, EB Docket No. 22-329 (filed July 30, 2025) (July 30, 2025 EPIC *Ex Parte*); Letter from Thomas M. Johnson, Jr. and Megan L. Brown, Wiley Rein LLP, to Marlene H. Dortch, FCC, EB Docket No. 22-329 (filed Aug. 4, 2025) (Aug. 4, 2025 CTIA *Ex Parte*); Letter from Thomas M. Johnson, Jr., and Megan L. Brown, Wiley Rein LLP, to Marlene H. Dortch, FCC, EB Docket No. 22-329 (filed Sept. 5, 2025) (Sept. 5, 2025 CTIA *Ex Parte*); Letter from Thomas M. Johnson, Jr., and Megan L. Brown, Wiley Rein LLP, to Marlene H. Dortch, FCC, EB Docket No. 22-329 (filed Sept. 5, 2025); Letter from Thomas M. Johnson, Jr., and Megan L. Brown, Wiley Rein LLP, to Marlene H. Dortch, FCC, EB Docket No. 22-329 (filed Sept. 10, 2025); Oct. 16, 2025 CTIA *Ex Parte*. Petitioners' and the Texas Association of Business's *ex parte* letters were in support of the Petition, while EPIC's were in opposition.

[66] Oct. 16, 2025 CTIA *Ex Parte* at 2-6.

enforcement, and the Commission have enabled some carriers to quickly share threat indicators with federal officials to promote a sector-wide response to cybersecurity threats as they occur.[67]

21. Specifically in response to the Salt Typhoon attacks, Petitioners explain that the sector partnered with the Federal Bureau of Investigation, National Security Agency, and CISA, which enabled agencies "to render technical assistance, rapidly share information to assist other potential victims, and work to strengthen cyber defenses across the commercial communications sector."[68] As a result of this collaboration, the federal government and its communications sector partners were able to share guidance that details specific tactics, techniques, and procedures used for initial exploitation, persistence, collection, and exfiltration; indicators of compromise and CVEs that were exploited; and threat hunting tips and specific mitigations that organizations are encouraged to implement to reduce the threat of Chinese state-sponsored and other advanced persistent threats.[69]

22. Petitioners also assert that carriers have taken steps to harden their networks in recent months based on what they learned from the Salt Typhoon attacks.[70] Some of the steps that providers have taken, where practical and commensurate with the risk, include implementing accelerated patching cycles, updating access controls, reviewing remote access configurations, improving threat hunting efforts, establishing log review processes and systems, disabling unnecessary outbound connections to limit lateral network movement, analyzing indicators of compromise, strengthening contractual obligations with third-party vendors, investing in zero trust approaches, and preparing for evolving threats.[71] Petitioners conclude that industry has voluntarily "devoted extensive personnel and resources to enhancing its cybersecurity posture in the wake of Salt Typhoon, and it will continue to do so to evolve its defenses as new threats emerge."[72]

III. DISCUSSION

A. Adoption of the Declaratory Ruling Was Unlawful and Unnecessary

23. We now conclude that adoption of the Declaratory Ruling was unlawful, because it adopted an erroneously broad reading of section 105 of CALEA and purported to assert the ability for the Commission to enforce this interpretation without adopting rules. The *Declaratory Ruling* was also ineffective because it failed to respond to the nature of the relevant cybersecurity threats and undermined the Commission's past agile and collaborative approach to cybersecurity. It is possible that the Commission erred in reaching its decision at least in part because it adopted it in a rushed manner just five days before a change of administration and without any public input.

---

[67] *Id.* at 6.

[68] *Id.* at 7 (citing FBI, Joint Statement from FBI and CISA on the People's Republic of China Targeting of Commercial Telecommunications Infrastructure (Nov. 13, 2024), https://www.fbi.gov/news/press-releases/joint-statement-from-fbi-and-cisa-on-the-peoples-republic-of-china-targeting-of-commercial-telecommunications-infrastructure).

[69] *Id.* at 8 (citing Press Release, National Security Agency/Central Security Service, NSA and Others Provide Guidance to Counter China State-Sponsored Actors Targeting Critical Infrastructure Organizations (Aug. 27, 2025), https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/4287371/nsa-and-othersprovide-guidance-to-counter-china-state-sponsored-actors-targeti/; CISA, Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System, https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-239a (Sept. 3, 2025)).

[70] *Id.* at 9-11.

[71] *Id.* at 9-10.

[72] *Id.* at 11.

1. The Declaratory Ruling misinterpreted CALEA

24. It was unlawful for the Commission to announce an interpretation of CALEA section 105 without adopting implementing rules. The Commission's role in implementing CALEA is limited as provided in the statute. In particular, the Commission lacks authority to enforce its view of what the statute independently requires. The Commission is charged with adopting rules to implement CALEA, particularly rules to address specific scenarios designated by Congress: (1) specific systems security and integrity requirements specified by section 229(b);[73] (2) cost recovery for compliance with section 103, as specified by section 229(e);[74] and, (3) in response to a petition, technical requirements or standards that satisfy the requirements of section 103 as provided in section 107(b).[75] Section 229(a) also provides more general authority to "prescribe such rules as are necessary to implement the requirements of [CALEA]," and section 229(d) provides that the Commission may enforce any such rules as violations of rules adopted under the Communications Act.[76] Absent rules, however, the Declaratory Ruling does not explain how the Commission could enforce CALEA's statutory provisions directly. Rather, section 108 of CALEA appears to commit authority to enforce the statutory requirements only to the courts.[77] By contrast, the Communications Act includes provisions explicitly authorizing the Commission to enforce not only its duly adopted rules but also the requirements of that Act itself.[78]

25. Indeed, the Commission recognized that its enforcement of CALEA depends on having adopted rules when, in 2006, it decided to codify the requirements of section 103 into part 1, subpart Z, of its rules.[79] The Declaratory Ruling did not explain how it could depart from this approach and enforce the CALEA statute directly. Even EPIC, in a memorandum supporting its opposition to the petition for reconsideration, can point only to CALEA's delegations of rulemaking authority to support Commission action in this area.[80] To the extent EPIC points to provisions in the Communications Act other than section 229 that may be relevant to cybersecurity,[81] it cannot justify a Declaratory Ruling that purports to

---

[73] *See* 47 U.S.C. § 229(b) (directing the Commission to adopt rules with specific provisions to implement section 105).

[74] *See* 47 U.S.C. § 229(e) (authorizing the Commission to grant a petition "to adjust charges, practices, classifications, and regulations to recover costs expended for making modifications to equipment, facilities, or services pursuant to the requirements of section 103").

[75] *See* 47 U.S.C. § 1006(b) (authorizing the Commission "to establish, by rule, technical requirements or standards" that meet the requirements of section 103 and other criteria).

[76] *See* 47 U.S.C. § 229(a), (d).

[77] 47 U.S.C. § 1007(a) ("A court shall issue an order enforcing this subchapter under section 2522 of title 18 only if the court finds that . . . ."); *see also* 18 U.S.C. § 2522.

[78] *See* 47 U.S.C. § 503(b) (prescribing penalties for, *inter alia*, "[a]ny person who is determined by the Commission … to have … willfully or repeatedly failed to comply with any of the provisions of this chapter or of any rule, regulation, or order issued by the Commission under this chapter").

[79] *Communications Assistance for Law Enforcement Act and Broadband Access and Services*, Second Report and Order and Memorandum Opinion and Order, 21 FCC Rcd 5360, 5390, para. 66 (2006) ("Accordingly, we find that, contrary to commenters who argued that authority to enforce CALEA lies exclusively with the courts under CALEA section 108, we have the authority to prescribe CALEA rules and investigate the compliance of those carriers and providers subject to such rules."); *id.* at 5389-90, paras. 64, 68 (deciding to adopt the requirements of section 103 as rules "in order to effectively enforce the statute").

[80] Electronic Privacy Information Center, In Support of the Commission's Declaratory Ruling (July 28, 2025), https://www.fcc.gov/ecfs/document/10730115135731/2, at 5-7 (EPIC Memorandum).

[81] *Id.* at 6-8 & n.39 (citing sections 201(b), 214, 222, 303, and 705 of the Communications Act of 1934, as amended, 47 U.S.C. §§ 201(b), 214, 222, 303, 605).

announce an interpretation of a statutory duty in CALEA, a separate statute. Section 229(c), also cited by EPIC, cannot provide appropriate justification because this section too requires the Commission first to have issued "regulations prescribed under this section."[82] Thus, the proper way for the Commission to implement CALEA is through notice-and-comment rulemaking, as it has done several times before, and not through a *sua sponte* Declaratory Ruling purporting to interpret the statute itself. Certain statements in the Declaratory Ruling also created vague obligations better suited for a rulemaking.

26. The Commission also erred in disregarding the limits imposed by the phrase "effected within its switching premises" in section 105 of CALEA. The Declaratory Ruling claimed that section 105 "affirmatively obligates carriers to take action to prevent *all* unauthorized interception and access to call-identifying information within their networks."[83] Though it acknowledged that section 105 refers only to interceptions and access that occur "within [a carrier's] switching premises" and noted the Commission's earlier recognition of that limitation,[84] it suggested instead that the obligation would apply to "their [entire] networks,"[85] without apparent limitation. As then-Commissioner Carr noted in dissent, the language of the Declaratory Ruling appears to "impos[e] an affirmative obligation on a covered provider to take certain undefined cybersecurity actions across every portion of their network—meaning, both within and outside the switching premises."[86] The Declaratory Ruling's statement that section 105 requires "[e]nterprise-level implementation" of cybersecurity practices[87] appears to go beyond the statute's clear reference to "within its switching premises."

27. The Declaratory Ruling also ignored a key limitation on CALEA's definition of "interception." The Declaratory Ruling noted that CALEA incorporates by reference the Wiretap Act's broad definition of "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."[88] The Commission reasoned that this expansive definition, combined with CALEA's use of the word "any," meant that section 105 reaches every unauthorized attempt to access a communications network, not just governmental interception efforts.[89] That approach ignores the construction that courts have consistently placed on the Wiretap Act's definition. As the Sixth Circuit has explained, the Wiretap Act is limited to communications intercepted contemporaneously with their transmission rather than data at rest.[90] The

[82] 47 U.S.C. § 229(c) ("The Commission shall review the policies and procedures submitted under subsection (b)(3) and shall order a common carrier to modify any such policy or procedure that the Commission determines does not comply with Commission regulations. The Commission shall conduct such investigations as may be necessary to insure compliance by common carriers with the requirements of the regulations prescribed under this section."); *see* EPIC Memorandum at 17.

[83] *Declaratory Ruling*, 40 FCC Rcd at 884, para. 13 (emphasis added).

[84] *See id.* at 884, para. 13 & n.45 (quoting *2019 Supply Chain Order*, 34 FCC Rcd at 11436, para. 35).

[85] *Declaratory Ruling*, 40 FCC Rcd at 884, para. 13.

[86] Dissenting Statement of Commissioner Carr, *available at* https://x.com/BrendanCarrFCC/status/1879674875973165368/photo/1.

[87] *Declaratory Ruling*, 40 FCC Rcd at 885, para. 14.

[88] 18 U.S.C. § 2510(4) (emphasis added); *see* 47 U.S.C. § 1001(1) incorporating by reference terms defined in 18 U.S.C. § 2510 and "the meanings stated in" that provision).

[89] *Declaratory Ruling*, 40 FCC Rcd at 884, para. 13.

[90] *Luis v. Zang*, 833 F.3d 619, 629 (6th Cir. 2016) (citing *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 113 (3d Cir. 2003), *as amended* (Jan. 20, 2004); *United States v. Steiger*, 318 F.3d 1039, 1048–49 (11th Cir. 2003); *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 878 (9th Cir. 2002)). *But see United States v. Councilman*, 418 F.3d 67, 79-80 (1st Cir. 2005) (casting doubt on the contemporaneity requirement, but ultimately concluding that the court "need not decide that question" on the facts of the case before it).

Declaratory Ruling's focus on the subject engaging in interception overlooks the more important object of the interception—namely, real-time communications, rather than information stored in providers' systems. The Declaratory Ruling's required "basic cybersecurity hygiene practices"—role-based access controls, changing default passwords, requiring minimum password strength, and adopting multifactor authentication—are all designed to thwart attempts to exfiltrate data on communications systems both in transit *and at rest*, thus reaching beyond section 105's limited focus on contemporaneous interception.[91] Nor does CALEA's narrow definition of "call-identifying information"—which encompasses only "dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier"[92]—require carriers to secure all information across their entire enterprises.

28. For these reasons, we find that the Declaratory Ruling was legally erroneous.

2. The Declaratory Ruling is ineffective at promoting cybersecurity

29. Salt Typhoon is a sophisticated nation-state hack by China targeting specific vulnerabilities, some of which are still being exploited. But the Declaratory Ruling, which broadly requires all telecommunications carriers to "take action to prevent all unauthorized interception and access to call-identifying information within their networks,"[93] offers no guidance about which particular vulnerabilities to prioritize or which at-risk information to protect, leaving carriers with a burdensome and inchoate compliance standard that does little to secure communications networks and protect national security. Moreover, the Declaratory Ruling applies the same inflexible, across-the-board cybersecurity requirements to all telecommunications carriers without regard to their risk, size, or organizational posture. This vague and amorphous standard risks imposing costly new burdens on many providers that are either not relevant to the potential threats they face, or which are redundant because those providers may already employ sufficient cybersecurity practices to reasonably reduce the risk of successful exploits by the most sophisticated threat actors. Reversing such policy is a separate and independent ground for rescinding the Declaratory Ruling. It also abandons the Commission's practice of working with industry to identify the areas of greatest security risk, offering guidance in reducing risk where possible, and adopting targeted, clear rules where necessary to secure networks.

30. Instead of taking the Declaratory Ruling's broad tack, we believe that the Commission should promote an agile and collaborative approach to cybersecurity as reflected in existing federal and state cybersecurity requirements and public-private partnerships that protect and secure communications networks. As Petitioners observe, communications providers "have long partnered with the federal government on its whole-of-government effort to secure critical infrastructure."[94] This collaborative approach to cybersecurity includes industry participation in the Comm-ISAC; the contribution of technical expertise to CSRIC; and collaboration with other federal agencies such as NIST and CISA to help produce best practices, guidelines, and tools to reduce cybersecurity risk.[95]

31. This flexible and coordinated approach has demonstrable benefits for the security of the communications sector. We agree with the Petitioners that "[t]he government-industry partnership model of collaboration has enabled communications providers to respond swiftly and agilely to Salt Typhoon, reduce vulnerabilities exposed by the attack, and bolster network cyber defenses in the future to deter repeat incursions."[96] According to Petitioners, the collaborative relationship between communications

[91] *Declaratory Ruling*, 40 FCC Rcd at 885, para. 14.

[92] 47 U.S.C. § 1001(2).

[93] *Declaratory Ruling*, 40 FCC Rcd at 884, para. 13.

[94] Oct. 16, 2025 CTIA *Ex Parte* at 4.

[95] *Id.* at 2-6.

providers and the federal government enabled some carriers to quickly share threat indicators related to the Salt Typhoon attacks with federal law enforcement agencies, who in turn were able to guide other carriers in taking steps to remove threat actors from their networks and harden them against future exploits.[97] Petitioners acknowledge that "Salt Typhoon and the related Volt Typhoon are nation-state, adversary-affiliated [advanced persistent threats] with unlimited resources against which private sector companies alone cannot defend themselves," and note that, since the attacks, some carriers have participated in regular briefings with the Commission and federal law enforcement and intelligence agencies to share information and promote a coordinated national response strategy.[98] In addition, some carriers have taken additional steps to harden their networks in recent months, including implementing accelerated patching cycles, updating access controls, reviewing remote access configurations, improving threat hunting efforts, disabling unnecessary outbound connections to limit lateral network movement, and strengthening contractual obligations with third-party vendors.[99]

32. Petitioners note that providers make these security improvements to their networks voluntarily and remain dedicated to bolstering security through their partnerships with the federal government.[100] As part of these efforts, they have made commitments that include leading providers establishing and actively participating in the Communications Cybersecurity Information Sharing and Analysis Center ("C2 ISAC"), "the next-generation Information Sharing and Analysis Center model designed to facilitate real-time threat intelligence sharing among members."[101] Providers have also established new intra-sector sharing and collaboration mechanisms, including a new forum for collaboration among Chief Information Security Officers from U.S. and Canadian providers, which they commit to expanding to other "like-minded countries" this autumn.[102] These commitments demonstrate that the federal government's collaborative approach to cybersecurity continues to be effective and that the inflexible and vague approach of the Declaratory Ruling is unnecessary.

33. Furthermore, the Commission is leveraging the full range of the Commission's regulatory, investigatory, and enforcement authorities to protect Americans and American companies from foreign adversaries, particularly the threats posed by the PRC and CCP, consistent with the whole-of-government approach. We are proceeding in separate dockets under clear and established statutory authorities to strengthen technology and telecommunications supply chains, to mitigate America's vulnerabilities to cyberattacks, espionage, and surveillance by foreign adversaries, and to ensure U.S. leadership in critical technologies. To highlight only some of those initiatives, we have adopted rules that require all applicants for submarine cable landing licenses to certify that they have created and will implement and update cybersecurity and physical security risk management plans;[103] adopted rules to ensure that foreign adversary controlled-test labs are not participating in the FCC's equipment

(Continued from previous page)

[96] *Id.* at 8.

[97] *Id.* at 6 (citing CISA, *Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System*, https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-239a (Sept. 3, 2025).

[98] *Id.*

[99] *Id.* at 9-10.

[100] *Id.* at 11.

[101] *Id.* at 7.

[102] *Id.*

[103] *See Submarine Cable Order/FNPRM* at 60-61, para. 105.

authorization program;[104] and are proposing to extend our equipment security rules to a larger class of foreign adversary-controlled devices.[105] In each instance, we promoted requirements for which we have clear legal authority that target specific adversaries and threats while developing and considering a record that allows us to weigh the costs and benefits of further regulation.

34. Had the Commission sought and considered public comment before adopting the Declaratory Ruling, it is possible that the agency would have understood that its proposed approach was overly broad, vague, and counterproductive. Its approach to cybersecurity failed to consider multiple aspects of the current and evolving cybersecurity landscape, including relevant best practices identified by CSRIC,[106] technical standards,[107] and industry security standards.[108] The Declaratory Ruling represented a drastic departure from data security standards, yet the Declaratory Ruling does not discuss this departure at all. The Declaratory Ruling also failed to consider less burdensome approaches, including collaboration between the federal government and industry, engaging with stakeholders who have experience and expertise in securing the nation's communications networks, or working to harmonize the Commission's cybersecurity expectations with existing best practices. In sum, the Declaratory Ruling was an ill-advised, rushed effort to take a controversial action without being grounded in a proper notice-and-comment process.

B. The NPRM Is Unnecessary

35. We also hereby rescind the NPRM that was adopted simultaneously with the Declaratory Ruling. The Commission adopted the NPRM on January 15, 2025, and released its text on its website on January 16, 2025, but has not published it (or a summary) in the Federal Register as would be required under the Administrative Procedure Act.[109] Therefore, the period for public comments never commenced,[110] and there is no record for the Commission to address here. Rather than promote a one-size-fits-all approach of a single rulemaking to govern all Commission licensees, we intend to continue to take the targeted approach to promoting effective cybersecurity protections discussed above. The NPRM in this proceeding is therefore unnecessary and will not be pursued.

IV. ORDERING CLAUSE

36. Accordingly, IT IS ORDERED that, pursuant to sections 1.106 and 1.108 of the Commission's rules, 47 CFR §§ 1.106, 1.108, and section 405(a) of the Communications Act of 1934, as

---

[104] *Promoting the Integrity and Security of Telecommunications Certification Bodies, Measurement Facilities, and the Equipment Authorization Program*, ET Docket No. 24-136, Report and Order and Further Notice of Proposed Rulemaking, FCC 25-27 (May 27, 2025).

[105] Press Release, FCC, FCC Approves New Safeguards Against Untrustworthy Gear (Oct. 28, 2025), https://docs.fcc.gov/public/attachments/DOC-415131A1.pdf.

[106] *See* CSRIC, FCC, *Communications Security, Reliability, and Interoperability Reports*, https://www.fcc.gov/CSRICReports (last visited Sept. 12, 2025).

[107] *See* 3GPP, TS Series 33: Security Aspects, https://rb.gy/x7e28z (last visited Sept. 15, 2025). 3GPP TS 33.126 through 33.128 specifically provide technical specifications for lawful intercept capabilities. *Id.*

[108] ISO, *ISO/IEC 27000 Family*, https://www.iso.org/standard/iso-iec-27000-family (last visited Sept. 12, 2025); *see* Telecommunications Industry Association, Quest Forum, SCS 9001 Supply Chain Security Management System Handbook (2023); ISACA, *COBIT*, https://www.isaca.org/resources/cobit (last visited Sept. 12, 2025); Center for Information Security, *CIS Critical Security Controls*, https://www.cisecurity.org/controls (last visited (Sept. 12, 2025).

[109] *See* 5 U.S.C. § 553(b) ("General notice of proposed rule making shall be published in the Federal Register . . . .").

[110] *See* 5 U.S.C. § 553(c) ("*After* notice required by this section, the agency shall give interested persons an opportunity to participate in the rule making through submission of written data, views, or arguments . . . ." (emphasis added)).

amended, 47 U.S.C. § 405(a), this Order on Reconsideration IS ADOPTED. The Declaratory Ruling and Notice of Proposed Rulemaking, FCC 25-9, 40 FCC Rcd 876 (Jan. 15, 2025), is RESCINDED and WITHDRAWN.

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary

STATEMENT OF
CHAIRMAN BRENDAN CARR

Re: Protecting the Nation's Communications Systems from Cybersecurity Threats, PS Docket No. 22-329

As the U.S. intelligence community has explained, Salt Typhoon—a China-sponsored advanced persistent threat group—infiltrated at least eight U.S. communications companies as part of a massive espionage campaign that affected dozens of countries. But Salt Typhoon was just the latest example in a decades-long history of foreign adversaries launching cyberattacks against our communications networks for both espionage and potential sabotage purposes.

In light of these ongoing risks, the U.S. government and the FCC, in particular, must act. But doing anything just so we can say we did something is not the answer. The FCC must take actions that are both lawful and effective. We have been doing exactly that at the FCC this year.

When I started as Chairman, one of the first actions I took was to stand up a new Council on National Security—a body that is staffed with experts that coordinate both within the FCC and across the intelligence community. We have withdrawn recognition for "bad labs" from our equipment authorization program for the first time. We have closed longstanding loopholes in our equipment security rules. We have adopted new security measures for submarine cables. And earlier this month, an FCC delegation traveled to London for a convening of Five Eyes telecom regulators to further our coordination on network security issues.

We have taken many more actions as well. Relevant to today's vote, the FCC has worked directly with carriers who have agreed to make extensive, coordinated efforts to harden their networks against a range of cyber intrusions. These have included accelerated patching of outdated or vulnerable equipment, updating and reviewing access controls, disabling unnecessary outbound connections, improving their threat-hunting efforts, and increasing cybersecurity information sharing.

All of these actions have been well within FCC legal authority and have effectively mitigated network vulnerabilities. In contrast, the Declaratory Ruling that we reconsider today was neither lawful nor effective.

It was unlawful because the FCC purported to read a statute that required telecommunications carriers to allow lawful wiretaps within a certain portion of their network as a provision that required carriers to adopt specific network management practices in every portion of their network. It was ineffective because it neither responded to the nature of the relevant cybersecurity threats nor was it consistent with the agile and collaborative approach to cybersecurity that has proven successful.

Indeed, when the prior Commission hastily rushed the item out the door just days before the presidential transition I said the following: "no[t] one official in the intelligence community has encouraged me to vote in favor of this FCC action. In fact, I was told that this type of FCC regulatory action at this moment would be counterproductive and deter the productive collaboration that is necessary today." Let me just reemphasize that here today. Biden-era cyber officials said at the time that the FCC's decision would not be merely ineffective—it would be counterproductive.

For these reasons, the Commission votes today to reverse that rushed and eleventh-hour approach to cybersecurity. In its place, we will continue our work to strengthen and harden the nation's communications networks and infrastructure.

For their great work on today's item, I want to thank Austin Randazzo, Leon Kenworthy, Scott Bouboulis, Josh Gehret, James Graves, Doug Klein, Hallie Laws, Zoe Li, and Zenji Nakazawa.

DISSENTING STATEMENT OF
COMMISSIONER ANNA M. GOMEZ

Re: Protecting the Nation's Communications Systems from Cybersecurity Threats, PS Docket No. 22-329

Salt Typhoon has been described as the worst telecommunications hack in our nation's history. It was a highly coordinated breach of American telecommunications infrastructure carried out by a foreign adversary that targeted American infrastructure, American companies, and American citizens, including the current President of the United States. But more importantly, it was a wake-up call. It showed us just how few incentives exist to force companies to address the vulnerabilities that allowed that attack to happen. And it proves to us that adversaries like the Chinese Communist Party (CCP) will not hesitate to act aggressively and decisively. And neither should we.

Sadly, the Commission today reverses the only meaningful effort this agency has advanced in response to that attack. The January Declaratory Ruling and Notice of Proposed Rulemaking were adopted because immediate action was needed at that time. They sought to create accountability, establish clear cybersecurity obligations, and put in place an enforceable framework to harden networks before the next breach. By rescinding those efforts and offering nothing in their place, the FCC leaves the country less safe at the very moment when these threats are increasing.

We're told the answer is not regulation, but voluntary collaboration. Collaboration is valuable and I support it as one part of a comprehensive cybersecurity strategy. However, collaboration is not a substitute for obligation. Handshake agreements without teeth will not stop state-sponsored hackers in their quest to infiltrate our networks. They won't prevent the next breach. They do not ensure that the weakest link in the chain is strengthened. If voluntary cooperation were enough, we would not be sitting here today in the wake of Salt Typhoon.

To be clear, partnership and collaboration are worthy goals. However, partnership and collaboration that carry no enforceable accountability are insufficient by design. Simply trusting industry to police itself is an invitation for the next breach. And when the next breach occurs, there will be no standards to measure compliance and no mechanism for determining which safeguards should have been in place. That is governing by hope rather than by duty, and the American public deserves better.

I will admit that going over this item was difficult. It read like a one-sided opposing statement, full of bombastic and unproven claims, rather than a level-headed approach to national security. But I found it curious that in it the FCC lists cybersecurity requirements that carriers already face under securities law, under state law, and in unrelated FCC rulemakings. To me, that list proves two points. First, this agency already accepts that requirements are sometimes necessary. Second, those requirements did not address the vulnerabilities that Salt Typhoon exploited. None of the actions cited in this item, like our work to secure undersea cables or the creation of an internal national security brainstorming group, would have prevented that attack. And nothing in this item would prevent the next one.

And the problem does not stop there. Ten months into this Administration, this FCC has still not put forward a single actionable solution to address the growing cybersecurity threat to our communications networks. Not one concrete proposal. Not one protection standard. Not one accountability mechanism. Today's decision is not a cybersecurity strategy. It is a hope and a dream.

This FCC also criticizes the Declaratory Ruling for not specifying which vulnerabilities should be prioritized, and for moving forward with what it calls a "partisan approach" that did not seek public input. If clarity and process were truly the concerns, then the solution should have been to strengthen the item through notice-and-comment and to provide companies with that clarity, not to discard the effort altogether. That is exactly why I proposed a bipartisan rulemaking process that would refine and perfect these requirements. That request, which would have continued this agency's bipartisan tradition of working together on national security issues, was declined.

Perhaps most concerning of all, the majority bases its decision on the assertion that the previous FCC action was unlawful. That is a statutory interpretation that does not stand to scrutiny. CALEA requires carriers to CALEA requires carriers to "ensure that any interception of communications or access to call-identifying information effected within its switching premises can be activated only in accordance with… lawful authorization."1 That provision therefore places an affirmative cybersecurity obligation on carriers, and the Communications Act gives the FCC authority to implement that obligation. In fact, I have noticed that many of the things the other side disagrees with tend to be simply labeled as "unlawful." Our recently upheld data breach notification rules are one clear example. You may disagree with the policy choice, but that disagreement does not erase that statutory authority. And I worry that this capricious attempt to label this tool as unlawful will hamstring this agency when it is inevitably called upon to respond to the next hack.

But rather than prepare this agency for that scenario, the Commission instead places its blind faith in a new collaborative approach. Yet this FCC does not explain what the approach is, what objectives it will pursue, what milestones it will track, or how the public will know whether it has succeeded. We are told that this internal council will help facilitate coordination, but the item does not describe how the council will translate its work into concrete steps to protect our telecommunications networks. This country cannot afford to wait for slow and cooperative progress that may never materialize.

That choice carries serious consequences. This FCC today is leaving Americans less protected than they were the day this breach was discovered. Salt Typhoon will not be the last attempt to infiltrate our networks, and without immediate action it will not be the last successful one.

History will remember whether we chose to act in the face of clear and imminent danger. The best time to do that was yesterday. The second-best time is now.

[1] 47 U.S.C. § 1004.

STATEMENT OF
COMMISSIONER OLIVIA TRUSTY

Re: *Protecting the Nation's Communications Systems from Cybersecurity Threats*, PS Docket No. 22-329, Order on Reconsideration (November 20, 2025).

Cybersecurity is national security. The Commission's responsibility to protect our nation's communications networks from foreign adversaries and other bad actors is one of our most important and urgent duties. The recent Salt Typhoon attacks underscore that our adversaries are sophisticated, well-resourced, and persistent, and that we must be equally strategic and agile in our response.

I support today's Order on Reconsideration because it course corrects and restores the Commission's focus on effective, collaborative, and legally sound action to strengthen network security. The Declaratory Ruling adopted earlier this year misconstrued the scope of the Communications Assistance for Law Enforcement Act and, in doing so, risked creating confusion rather than clarity about the obligations of service providers. By rescinding that ruling and withdrawing the related Notice of Proposed Rulemaking, we affirm our commitment to act within the bounds of our statutory authority and to pursue cybersecurity protections that are both targeted and enforceable.

Importantly, today's decision does not signal a retreat from our cybersecurity mission. On the contrary, it reflects a recognition that one of the most effective defenses against foreign threats comes from a dynamic partnership between the federal government and the private sector. Over the past several months, providers have stepped up with meaningful, voluntary measures to harden their networks, and the Commission will continue to hold them accountable through ongoing monitoring, enforcement, and future rulemakings where appropriate.

Cybersecurity is not a one-time task. It is a continuous effort that demands vigilance, innovation, and collaboration. I look forward to continuing to work with my colleagues, our federal partners, and industry leaders to secure America's communications systems and safeguard the public trust.

Thank you to the Public Safety and Homeland Security Bureau for their work on this item.