from circumstances outside of the cable operator's control (including failed retransmission consent or program carriage negotiations during the last 30 days of a contract), in which case notice shall be provided as soon as possible using any reasonable written means at the operator's sole discretion, including channel slates. Notice of rate changes shall include the precise amount of the rate change and explain the reason for the change in readily understandable terms. Notice of changes involving the addition or deletion of channels shall individually identify each channel affected.

47 CFR 76.1603(c) states that a cable operator not subject to effective competition shall provide 30 days' advance notice to its local franchising authority of any increase proposed in the price to be charged for the basic service tier.

47 CFR 76.1619(b) states in case of a billing dispute, the cable operator must respond to a written complaint from a subscriber within 30 days. The required response may be delivered by email, if the consumer used email to make the request or complaint directly to the cable operator, or if the consumer specifies email as the preferred delivery method in the request or complaint.

47 CFR 76.1619(c) states a cable franchise authority may enforce the customer service standards set forth in this section against cable operators. The franchise authority must provide affected cable operators 90 days written notice of its intent to enforce standards.

47 CFR 76.1600 permits written information provided by cable operators to subscribers or customers pursuant to Sections 76.1601, 76.1602, 76.1603, 76.1604, 76.1618, and 76.1620, as well as subscriber privacy notifications required by cable operators, satellite providers, and open video systems pursuant to Sections 631, 338(i), and 653 of the Communications Act, to be delivered by email if certain consumer safeguards are met, as set forth in Section 76.1600(a) and Section 76.1600(b).

Section 76.1600(c) permits cable operators to provide certain portions of the Section 76.1602 annual notices electronically to subscribers who have not opted out of electronic delivery under Section 76.1600(a)(3) or 76.1600(c)(3) if they prominently display the following on the front or first page of the printed annual notice:

(1) A weblink in a form that is short, simple, and easy to remember, leading to written information required to be provided pursuant to Section 76.1602(b)(2), (7), and (8);

(2) A weblink in a form that is short, simple, and easy to remember, leading to written information required to be provided pursuant to Section 76.1602(b)(5); and

(3) A telephone number that is readily identifiable as an opt-out mechanism that will allow subscribers to continue to receive paper copies of the entire annual notice.

47 CFR 76.1600(d) provides that, if the conditions for electronic delivery in subsections 76.1600(a) and 76.1600(b) are not met, or if a subscriber opts out of electronic delivery, the written material must be delivered by paper copy to the subscriber's physical address.

Federal Communications Commission.

Marlene Dortch,

Secretary.

[FR Doc. 2025–22714 Filed 12–12–25; 8:45 am]

BILLING CODE 6712–01–P

FEDERAL COMMUNICATIONS COMMISSION

[PS Docket No. 22–329; FCC 25–81; FR ID 322072]

Protecting the Nation's Communications Systems From Cybersecurity Threats

AGENCY: Federal Communications Commission

ACTION: Notice; order on reconsideration.

SUMMARY: In this document, the Federal Communications Commission (''Commission'' or ''FCC'') announces that it has reconsidered and rescinded a prior Declaratory Ruling and Notice of Proposed Rulemaking, neither of which had been published in the **Federal Register**. The Declaratory Ruling misconstrued the Communications Assistance for Law Enforcement Act (CALEA), and the Notice of Proposed Rulemaking was based in part on the Declaratory Ruling's flawed legal analysis and proposed ineffective cybersecurity requirements. This Order follows the FCC's engagement with providers to help strengthen their cybersecurity posture.

DATES: The Order on Reconsideration was adopted on November 20, 2025.

FOR FURTHER INFORMATION CONTACT: Leon T. Kenworthy, Cybersecurity and Communications Reliability Division, Public Safety and Homeland Security Bureau, at *Leon.Kenworthy@fcc.gov* or at (202) 418–1886.

SUPPLEMENTARY INFORMATION: This is a summary of the Commission's Order on Reconsideration, in PS Docket No. 22–329; FCC 25–81, adopted on November 20, 2025 and released on November 21, 2025. The full text of this document is available online at *https://docs.fcc.gov/public/attachments/FCC-25-81A1.pdf.* The full text of this document is also available for inspection and copying during business hours in the FCC Reference Center, 45 L Street NE, Washington, DC 20554. To request materials in accessible formats for people with disabilities, send an email to *FCC504@fcc.gov* or call the Consumer & Governmental Affairs Bureau at 202–418–0530 (voice).

Synopsis

I. Introduction

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. As part of its efforts to do so, the FCC stood up a new Council on National Security within the agency earlier this year, and we have been working with network providers since the beginning of the year.

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. In particular, through a collaborative approach, providers have agreed to implement additional cybersecurity controls to harden their networks. 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. Providers have also committed to increased cybersecurity information sharing, both with the federal government and within the communications sector. This represents a significant change in cybersecurity practices compared to the measures in place in January.

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. 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.

Second, and for similar reasons, we are withdrawing the Notice of Proposed Rulemaking (NPRM) that accompanied the Declaratory Ruling. 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

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, 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. 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.

Congress created the Commission, among other reasons, ''for the purpose of the national defense . . . .'' 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

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. 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'' and ''mitigate America's vulnerabilities to cyberattacks, espionage, and surveillance by foreign adversaries.'' 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 the public and the public safety community about a recent outage that reportedly resulted from a ransomware attack.

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. 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.

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.'' 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. 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.

B. Other Communications Sector Cybersecurity Measures

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, as part of registration statements, annual reports, and other filings. Public companies must also disclose 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. Additionally, many carriers are subject to state laws that require them to implement reasonable cybersecurity risk management practices to protect customer data. 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, including those in critical infrastructure sectors like communications. CISA sought comment on cyber incident reporting requirements in June 2024 and has indicated it expects to adopt a final rule in May 2026.

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. 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. 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. CISA also provides voluntary tools and services to aid in strengthening cybersecurity practices, including the Cybersecurity Performance Goals (CPGs), which are baseline practices that critical infrastructure entities can use to manage and reduce cybersecurity risks. CISA's cross-sector CPGs provide sector-agnostic, prioritized guidance to help organizations focus resources on the most effective risk-reduction measures. To support CPG adoption, CISA offers Assessment Training with regional cybersecurity experts to help communications providers better understand the CPGs and cybersecurity risk assessment. 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.''

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

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.'' 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.'' Among those responsibilities is the duty to adopt rules to implement the ''systems security and integrity'' obligations of section 105 of CALEA. 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. The Commission has also cited these duties in adopting other rules directed at preventing carriers from allowing unauthorized surveillance within their networks.

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. 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 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.'' 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.

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. 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'' and as including facilities-based broadband internet access service (BIAS) providers and interconnected Voice over internet Protocol (VoIP) service providers.

D. January 2025 Declaratory Ruling and Notice of Proposed Rulemaking

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.'' 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.'' 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.'' 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.''

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 their communications systems and services,'' such as ''implementing role-based access controls, changing default passwords, requiring minimum password strength, and adopting multifactor authentication.'' 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.'' 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.

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. The Declaratory Ruling was effective immediately.

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. 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. 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 Providers. 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.

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.[1] On February 28, 2025, the Electronic Privacy Information Center (EPIC) filed an Opposition to the Petition. Petitioners submitted a reply on March 10, 2025. Petitioners, EPIC, and the Texas Association of Business subsequently submitted *ex parte* filings.

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. According to Petitioners, these forums and other collaborative activities involving CISA, federal law 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.

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.'' 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.

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. 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. 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.''

III. Discussion

E. Adoption of the Declaratory Ruling Was Unlawful and Unnecessary

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.

1. The Declaratory Ruling Misinterpreted CALEA

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); (2) cost recovery for compliance with section 103, as specified by section 229(e); and, (3) in response to a petition, technical requirements or standards that satisfy the requirements of section 103 as provided in section 107(b). 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. 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. 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.

[1] 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.

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. 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. To the extent EPIC points to provisions in the Communications Act other than section 229 that may be relevant to cybersecurity, it cannot justify a Declaratory Ruling that purports to 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.'' 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.

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.'' 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, it suggested instead that the obligation would apply to ''their [entire] networks,'' 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.'' The Declaratory Ruling's statement that section 105 requires ''[e]nterprise-level implementation'' of cybersecurity practices appears to go beyond the statute's clear reference to ''within its switching premises.''

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.'' 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. 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. The 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. 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''—require carriers to secure all information across their entire enterprises.

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

2. The Declaratory Ruling Is Ineffective at Promoting Cybersecurity

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,'' 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.

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.'' 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.

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.'' According to Petitioners, the collaborative relationship between communications 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. 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. 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.

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. 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.'' 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. 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.

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; adopted rules to ensure that foreign adversary controlled-test labs are not participating in the FCC's equipment authorization program; and are proposing to extend our equipment security rules to a larger class of foreign adversary-controlled devices. 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.

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, technical standards, and industry security standards. 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.

F. The NPRM Is Unnecessary

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. Therefore, the period for public comments never commenced, 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

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 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 Dortch,

Secretary.

[FR Doc. 2025–22830 Filed 12–12–25; 8:45 am]

BILLING CODE 6712–01–P

FEDERAL COMMUNICATIONS COMMISSION

[DA 25–1009; FR ID 322148]

Notice Debarment; Federal Lifeline Program

AGENCY: Federal Communications Commission.

ACTION: Notice.

SUMMARY: The Enforcement Bureau (the ''Bureau'') permanently debars Q Link from the federal Lifeline program (Lifeline Program) and all federal universal service support mechanisms.

DATES: Debarment commences on the date Q Link receives the debarment letter or December 15, 2025, whichever date comes first.

ADDRESSES: Federal Communications Commission, Enforcement Bureau, Investigations and Hearings Division, 45 L Street NE, Washington, DC 20554.

FOR FURTHER INFORMATION CONTACT: Christopher Sova, Federal Communications Commission, Enforcement Bureau, Investigations and Hearings Division, 45 L Street NE, Washington, DC 20554. Christopher Sova may be contacted by phone at (202) 418–1868 or by email at *Christopher.Sova@fcc.gov.*

SUPPLEMENTARY INFORMATION: The Bureau debars Q Link from the federal