Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Public Safety and Homeland Security Bureau Requests Comment on Implementation of Signaling System 7 Security Best Practices	)))	PS Docket No. 18-99

COMMENTS OF CTIA

Thomas C. Power
Senior Vice President, General Counsel

Scott K. Bergmann
Senior Vice President, Regulatory Affairs

Thomas K. Sawanobori
Senior Vice President, Chief Technology Officer

Melanie K. Tiano
Director, Cybersecurity and Privacy

CTIA
1400 Sixteenth Street, NW, Suite 600
Washington, DC 20036
(202) 736-3200

May 3, 2018

Table of Contents

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Public Safety and Homeland Security Bureau Requests Comment on Implementation of Signaling System 7 Security Best Practices	)))	PS Docket No. 18-99

COMMENTS OF CTIA

I. INTRODUCTION AND SUMMARY

CTIA[1] submits these comments in response to the Federal Communications Commission's ("FCC" or "Commission") Public Notice seeking information on communications service providers' implementation of Signaling System 7 ("SS7") security best practices.[2] CTIA is pleased to share with the Commission information about SS7 and the U.S. industry's work.

SS7 is the global standard signaling protocol used by carriers to support call setup, routing, and exchange, allowing customers to roam between carriers. As the world of mobile communications has grown in coverage, networks, and participants, so too has the number of carriers with access to SS7 networks. This expanded access has resulted in an increased risk of possible exploitation of the SS7 network by bad actors. The wireless industry has taken concrete

[1] CTIA® (www.ctia.org) represents the U.S. wireless communications industry and the companies throughout the mobile ecosystem that enable Americans to lead a 21st- century connected life. The association's members include wireless carriers, device manufacturers, suppliers as well as apps and content companies. CTIA vigorously advocates at all levels of government for policies that foster continued wireless innovation and investment. The association also coordinates the industry's voluntary best practices, hosts educational events that promote the wireless industry, and co-produces the industry's leading wireless tradeshow. CTIA was founded in 1984 and is based in Washington, D.C.

[2] Public Notice, Public Safety and Homeland Security Bureau Requests Comment on Implementation of Signaling System 7 Security Best Practices, DA 18-333, PS Docket No. 18-99 (April 3, 2018) ("PN").

action, often in concert with government and stakeholders around the world, to address SS7 security risks.

The FCC's Communications Security, Reliability, and Interoperability Council ("CSRIC") Working Group on Legacy Systems Risk Reduction, composed of wireless industry stakeholders, technology experts, and federal government participants, studied the risks associated with SS7 and developed nine recommendations to reduce SS7 security risks and increase situational awareness.[3] The recommendations applied to various parts of the wireless ecosystem and fell into two categories: 1) awareness of SS7 signaling risks and 2) security best practices for SS7 communications.[4] In addition to executing against the CSRIC recommendations, carriers daily use sophisticated tools to mitigate security risks. Standards groups also have supported best practices and risk mitigations, such as end user device- and application-based encryption, which are effective and widely available to augment security.

As these comments explain, carriers are using the CSRIC Report's recommendations and other best practices to mitigate threats to their networks. Barriers do exist and work should continue to facilitate global security improvements, particularly among the non-carrier and non-U.S. ecosystem participants like aggregators and foreign carriers and governments. U.S. carriers have successfully engaged with some aggregators to help address the threats to SS7. Going forward, the Commission should engage with the Department of Homeland Security ("DHS") and other stakeholders to collectively meet challenges; public proceedings are not well-suited to a fulsome discussion of network security risks and mitigations because bad actors are constantly

[3] *See* CSRIC V: Working Group 10, Legacy Risk Reductions (2017), https://www.fcc.gov/files/csric5-wg10-finalreport031517pdf ("CSRIC Report").

[4] Public Notice, FCC's Public Safety and Homeland Security Bureau Encourages Implementation of CSRIC Signaling System 7 Security Best Practices, 32 FCC Rcd 6669 (2017).

looking for information they can exploit. Cooperation and better sharing of declassified information in a confidential setting is critical to reducing vulnerabilities and addressing new security threats as they emerge. The private sector needs to have access to information about emerging threats, and should be able to share information on a confidential basis with others in the ecosystem that may need to take action as well.

II. INDUSTRY HAS BEEN WORKING COLLABORATIVELY WITH THE FEDERAL GOVERNMENT TO ADDRESS SS7 ISSUES.

The global SS7 network was designed decades ago as a carrier-only network where trusted carriers safeguarded their credentials to access the network. For decades, the "carrier trust model" worked because of the limited number of participants involved. Problems have arisen from expanding SS7 access to a large number of carriers around the world. As one carrier put it, "the growing number of carriers having *legitimate* credentials into the network creates the threat to SS7."[5] U.S. carriers handle tens of billions of SS7 messages daily, the overwhelming majority of which are legitimate communications. To strike the appropriate balance between caution and connectivity, industry has taken an aggressive but measured approach as it implements solutions to address SS7 threats while avoiding collateral impacts to subscribers and the risk of blocking legitimate traffic.

The CSRIC's work on SS7 showed how important collaboration is among industry stakeholders and government. The CSRIC Report's recommendations were based on industry and government expertise, with participants working together for months to identify the relevant issues and determine what steps would best mitigate the potential of SS7 exploits. The CSRIC

[5] Letter from Timothy McKone, AT&T Services, to Senator Ron Wyden at 1 (Oct. 13, 2017) https://www.wyden.senate.gov/imo/media/doc/ATT%20SS7%20Response.pdf ("AT&T Sen. Wyden Letter")

working group included internet service providers, mobile operators, and others like Oracle, iConnectiv, Nsight, and Seculore Solutions LLC. It included the valuable participation of DHS, the National Institute of Standards and Technology ("NIST") and the FCC. And it drew on leading subject matter experts from Nokia Bell Labs, Security Research Labs, and Adaptive Mobile.

The CSRIC effort built on the work of the international association GSMA, which has issued security best practices and guidelines.[6] CSRIC observed that carriers around the world play a role, as do aggregators that provide wholesale SS7 interconnection capabilities and "have a wider view of signaling traffic originating from domestic and international entities and terminating in the U.S. telecommunications network."[7]

In addition to collaboration in CSRIC, the mobile industry has directly engaged with DHS on these and broader security issues. As the CSRIC Report explained, several DHS components partner with the private sector. DHS is the sector-specific agency for the communications sector and regularly interacts with the Communications Sector Coordinating Council ("CSCC").[8] DHS hosts the National Cybersecurity and Communications Integration Center ("NCCIC") in which many carriers are embedded, facilitating real-time detection, response and information-sharing. Many CTIA members participate in DHS information sharing programs including the National Security Information Exchange ("NSIE") and Cyber Information Sharing & Collaboration Program ("CISCP"). In addition, DHS representatives

[6] *See* GSMA, Fraud and Security Group, https://www.gsma.com/aboutus/leadership/committees-and-groups/working-groups/fraud-security-group (last accessed Apr. 20, 2018).

[7] CSRIC Report at 13.

[8] Communications Sector Coordinating Council, https://www.comms-scc.org/.

regularly participate in CTIA's Cybersecurity Working Group meetings. Carriers have met individually and collectively with staff at DHS to discuss particular concerns and possible exploits. One lesson learned from those interactions is the need, described below, for additional sharing by the government of unclassified information. Carriers cannot solve this challenge alone, and they cannot make as much progress as they would like if the government does not share actionable information with relevant stakeholders regarding what may be of greatest or imminent concern.

III. THE FCC SHOULD BE ENCOURAGED BY INDUSTRY'S AGGRESSIVE EFFORTS TO ADDRESS SS7 ISSUES.

The wireless industry has been executing against the CSRIC report's recommendations and taking related measures to minimize SS7 risks.[9] Work must continue to reduce barriers to implementation, particularly regarding information sharing, and to encourage progress by non-carrier, global ecosystem participants.

A. The CSRIC Report identified important recommendations.

The Working Group conducted an assessment of the risks to carriers, individual subscribers, and critical infrastructure services from bad actors exploiting global SS7 signaling infrastructures. It issued a report on risks and followed up with recommendations. CSRIC offered nine key recommendations for industry:

- CSRIC recommended that "industry continue to implement signaling interconnection monitoring and filtering."[10] Carriers are doing this constantly and dynamically.
- CSRIC endorsed the GSMA best practices and recommended continued advancements in sharing of threat intelligence.[11] Carriers are doing this, including by using GSMA SS7

[9] *See*, CTIA, *CTIA Statement on SS7 and FCC CSRIC Recommendations* (https://api.ctia.org/docs/default-source/default-document-library/ss7-statement-2017-final.pdf).

[10] CSRIC Report at 18.

[11] *Id*.

firewall rules, FS.11, IR.82 (as applicable) and other standards, and by sharing information in several venues.

- CSRIC addressed the role of aggregators, recommending that industry engage signaling aggregators in efforts to address overall security, monitoring and filtering.[12] Carriers are working with aggregators, who play an important role given their broad view of global wireless telecommunication traffic.

- CSRIC emphasized information sharing. "The CSRIC recommends that the industry continue to leverage and expand the existing threat information sharing resources" and work with the DHS National Coordinating Center for Communications ("NCC") and in the Communications Information Sharing and Analysis Center ("Comm-ISAC").[13] Industry does this daily and is constantly engaged with DHS and each other.

- CSRIC urged industry to continue work on the automated threat info-sharing pilot through CTIA.[14] That pilot has concluded after robust participation from a cross-sector of industry participants. It provided a proof of concept and validated the concern that the DHS Automated Indicator Sharing Portal is not ideally suited to telecom-specific use cases. CTIA and its members are evaluating how to leverage the pilot and not duplicate or dilute other effective information-sharing channels.

- CSRIC recommended continued steps to adapt the GSMA efforts to protect Diameter and overall 5G.[15] The global mobile sector is advancing security in 5G in numerous standard bodies, which includes further work at GSMA and in many other venues, from IETF to 3GPP.

- CSRIC recommended that industry "continue to explore" future work on Circles of Trust.[16] The CSRIC report observed that "the 3GPP is studying the concept of trust groups among telecommunications carriers."[17] However, CSRIC also noted that "[f]orming trust groups across as many upstream and downstream interfaces as possible could be very beneficial, but it is unrealistic to expect global trust and adoption across different types of operators, exchange operators and third party service providers."[18] As explained below, this observation was prescient as global challenges are stalling progress.

- CSRIC urged ongoing security assessment of signaling infrastructure "to detect and mitigate possible threat vectors."[19] Carriers and others regularly review traffic patterns, networks, infrastructure, and other aspects of security.

[12] *Id*.

[13] *Id*.

[14] *Id*.

[15] *Id*. at 18-19.

[16] *Id*. at 19.

[17] *Id*. at 14.

[18] *Id*.

[19] *Id*. at 19.

- CSRIC recommended that "industry encourage the use of available encryption technologies," and noted that encryption may have particular utility for a "VIP or key government official."[20] CTIA and carriers promote available tools that can help users layer on security.[21]

The FCC last year released a Public Notice urging use of the CSRIC recommendations.[22] U.S. carriers and others have been doing so, as described briefly above, and CTIA is happy to provide more detail below in response to the FCC's questions.

B. Carriers are advancing the CSRIC recommendations using best practices and sophisticated tools.

Global communications service providers dynamically balance the risk of blocking legitimate communications against the security risks associated with malicious abuse of legitimate credentials, while recognizing that there is no one-size-fits-all solution for all carriers and platforms. This concept was central to the CSRIC Report, which gave industry flexibility to implement best practices as appropriate to their organizations.

Carriers have been thinking about SS7 and how to protect the networks for years. That said, once recommendations were released, carriers determined how best to implement those recommendations, where feasible, given the uniqueness of each network. For example, carriers using CDMA networks found that not all recommendations related to GSMA network best

[20] *Id*. at 17.

[21] *See, e.g.* CTIA, *Consumer Resources, Protecting Your Data*, https://www.ctia.org/consumer-resources/protecting-your-data (CTIA recommends that consumers "[u]se additional layers of security—like Virtual Private Networks (VPNs) and encryption applications—to further protect your sensitive information, especially on open networks.").

[22] Public Notice, FCC's Public Safety and Homeland Security Bureau Encourages Implementation of CSCRIC Signaling System 7 Security Best Practices, 32 FCC Rcd 6669 (2017).

practices were applicable.[23] Carriers also analyzed their risk management approach and considered how to address SS7 risks in that broader context; as one national carrier explained, "Sprint will continue to evaluate and adopt relevant industry best practices, as well as assess and deploy new security tools and enhancements as part of its ongoing security program review."[24]

Once carriers analyzed and customized the recommendations, they set to work on implementation. The four nationwide carriers have implemented or are advancing all of the CSRIC recommendations. Small and medium-size carriers are implementing them as appropriate to their organizations. As implementation continues, small and medium carriers also benefit from the network improvements resulting from the larger carriers' adoption.

Carriers are currently engaging in filtering and network monitoring to combat the risk of SS7 network exploits. This is no small task. The volume of communications that traverse U.S. networks is staggering. To take just one aspect of one carrier's experience, security experts see more than 30 billion vulnerability scans and 400 million spam messages cross its network every day; and 5 billion vulnerability scans and 200,000 malware events targeted at its network every

[23] *See, e.g.*, Letter from Vonya B. McCann, Sprint, to Senator Ron Wyden at 3 (Oct. 13, 2017) https://www.wyden.senate.gov/imo/media/doc/Sprint%20Response%20to%20Wyden%20SS7%20Letter.pdf ("Sprint Sen. Wyden Letter") ("Because Sprint is a CDMA carrier, not all GSMA SS7 best practices are applicable to Sprint."); *see generally* Letter from Robert S. Fisher, Verizon, to Senator Wyden Letter (Oct. 13, 2017) at 1 https://www.wyden.senate.gov/imo/media/doc/Verizon%20SS7%20Letter.pdf ("Verizon Sen. Wyden Letter") (noting that because it uses a CDMA mobile network, that network "is less susceptible to SS7 attacks than networks using the GSM standard").

[24] Sprint Sen. Wyden Letter at 3.

day.[25] Among their tools, carriers have found that SMS home routing,[26] home network monitoring, authentication, and the ability in 5G to encrypt International Mobile Subscriber Identity information have been particularly helpful. The industry is also looking to constantly refine approaches. To this end, the global wireless industry is looking ahead to next generation networks, such as 5G, and building layered security into the accompanying protocols.

C. Some barriers remain, particularly with respect to non-carrier actors.

The Commission asks about the barriers communications providers have encountered in implementing the recommendations.[27] Industry participants' experience has revealed a few obstacles, some of which will persist.

First, SS7 challenges are global, as attempted exploits to date have mainly come from overseas operators and actors. Even though domestic carriers are actively guarding against SS7 network threats, global cooperation is essential. Difficulties in securing international cooperation have made it very challenging to make progress on the CSRIC recommendation to establish Circles of Trust. This was anticipated by CSRIC and is not a surprise. Peering agreements with international carriers can be complex and challenging to negotiate, so there is

[25] Chris Boyer, *How the Public Safety Bureau Paper Gets Cybersecurity* Wrong, AT&T Public Policy Blog (Jan. 25, 2017), https://www.attpublicpolicy.com/cybersecurity/how-the-public-safety-bureaupaper-gets-cybersecurity-wrong/.

[26] *See, e.g.*, Sprint Sen. Wyden Letter at 2 ("Sprint has implemented SMS Home Routing."); *id*. at 3 ("Sprint will continue to evaluate and adopt relevant industry best practices, as well as assess and deploy new security tools and enhancements as part of its ongoing security program review."); AT&T Sen. Wyden Letter at 2 ("We have also implemented 'SMS Home Routing.'"); Verizon Sen. Wyden Letter at 1 ("Verizon's commitment to our network security includes . . . home routing on the SMS platform"); Letter from Anthony Russo, T-Mobile, to Senator Ron Wyden, at 4 (Oct. 13, 2017) https://www.wyden.senate.gov/imo/media/doc/10-13%20%20T%20Mobile%20Response.pdf ("T-Mobile Sen. Wyden Letter") ("T-Mobile has implemented 'SMS Home Routing.'").

[27] PN at 2.

no simple solution to export U.S. SS7 strategies abroad. Nevertheless, U.S. industry continues to work with global organizations like GSMA to expand collaboration and trusted relationships, because that is key to addressing SS7 and future security challenges. FCC and other United States government promotion of these imperatives overseas would help.

Second, there remain barriers to information sharing. As a recent CSRIC report noted, there are "capacity, accuracy, quality, timeliness, and issues resulting from a lack of consistent, standard formats and accepted nomenclature that should be used to share information."[28] Indeed, CSRIC noted that "[t]he most cited technical impediment to sharing could be broadly characterized as a lack of 'standardization' of formats and technology."[29] For example, the Trusted Automated Exchange of Indicator Information (TAXII) and Structured Threat Information Expression (STIX) protocols designed to standardize cyberthreat information do not currently support telecom-specific nomenclature. The U.S. wireless sector is looking at and trying to solve these challenges by discussing and developing standards, tools, protocols, and best practices recommendations, among other efforts.

Information sharing barriers may be more challenging for small and medium sized carriers as CSRIC's work on cybersecurity recognizes.[30] These providers play an important role in the vibrant mobile marketplace, as their size often gives them the agility to innovate to meet consumer needs. "[A]t small compan[ies] employees often wear many different hats, and as

[28] CSRIC 5, Working Group 5, Cyber Security Information Sharing Final Report at 15 (Mar. 2017) https://www.fcc.gov/files/csric5-wg5-finalreport031517pdf ("CSRIC Information Sharing Report"). "Similarly, rectifying differing terminology for the same piece of information as it is shared causes confusion, adds time, and lessens the effectiveness of information sharing." *Id.*

[29] *Id.*

[30] *See* CSRIC IV, Working Group 4, Cybersecurity Risk Management and Best Practices: Final Report (2015) ("CSRIC Cyber Report") at 204.

such, the company may suffer from a lack of internal resources with the time and technical skill sets required to contribute to the larger information-sharing environment."[31] Monetary resources are also a factor, as "[b]uilding requisite sharing infrastructure, buying a data feed, and dedicating human resources are all cost centers."[32] Small and medium sized carriers may not be able to dedicate an employee, let alone a team, to engage in information sharing, despite the company's willingness to participate in such efforts.[33] The government can consider incentives for small and medium sized companies to participate in information sharing and to advance their overall security. In particular, the government should consider focusing resources on building use cases at NIST and elsewhere. This is something the communications sector has long urged.[34]

Finally, the potential for liability and unwarranted public disclosures remain an impediment to broader sharing. In the past, "[l]ack of legal clarity on the civil front, and the potential for criminal sanctions . . . led companies to take a conservative approach to information sharing."[35] Uncertainties remain about the scope of protections under the Cybersecurity Information Sharing Act of 2015 ("CISA") from antitrust liability and concerns persist about the potential availability of information in civil discovery,[36] such as from subpoenas to ISACs.[37]

[31] CSRIC Information Sharing Report at 15.

[32] *Id.* at 17.

[33] *See id.* at 6.

[34] *See, e.g.*, Communications Sector Coordinating Council letter to GAO, October 2017 ("government efforts, like those at NIST, might focus on this segment [small business] with use cases and other work, instead of regularly updating existing documents or promulgating new guidance.") https://docs.wixstatic.com/ugd/0a1552_ab65e31fbff94f85a6b8c31420ab1503.pdf

[35] CSRIC Information Sharing Report at 6.

[36] *See id.* at 17.

[37] *See, e.g.*, Testimony of Denise Anderson On Behalf of the National Health Information Sharing & Analysis Center and the National Council of Information Sharing and Analysis Centers Before the United States House of Representatives Committee on Energy and Commerce on *Cybersecurity in the Health Care Sector: Strengthening Public-Private Partnerships* (April 4,

Relatedly, the government needs to share more information with carriers outside a classified setting. If new and emerging security threats are classified, carriers may be unable to share the information with all pertinent parties, such as suppliers. For threat information to be actionable by the wireless industry, there needs to be greater sharing of declassified information. Further, if the government has information about a risk or exploit, carriers and others in the ecosystem need to know about it as soon as possible so they can begin to respond. This concern has been discussed with DHS personnel, who indicate they are committed to addressing it. The government should not over-classify information that is actionable and appropriate for sharing with industry.

IV. EVALUATION OF SUCCESS IS ONGOING AS EACH CARRIER DYNAMICALLY ADDRESSES SECURITY.

The Commission seeks comment on evaluation of the implementation of the CSRIC Report's SS7 recommendations.[38] So far, the carriers' implementations of many of the CSRIC Report's recommendations have been successful in reducing SS7 risks. It is important to remember that SS7 is one of many global threats that industry dynamically addresses. Carriers evaluate the effectiveness of their many network protection measures using a variety of tools.

While no security strategy is foolproof, carriers' network security practices are effective. The U.S. wireless network is quite secure, particularly compared to overseas networks. A cybersecurity expert testified before Congress that "the United States has the most secure

2017) (describing concerns about a "non-party deposition subpoena to furnish all documentation related to communications between the Auto ISAC and one of its members' as the sort of thing that if successful would "effectively kill information sharing") available at https://www.hsdl.org/?view&did=801227

[38] PN at 2.

wireless infrastructure in the world."[39] This is, in part, because the carriers that manage domestic networks have relatively little roaming as compared to the rest of the world. Another factor minimizing the risk of an SS7 attack is the fact that, as a general matter, SS7 exploits are not suitable for general, large scale attacks. While the SS7 network can be exploited by sophisticated actors to target particular persons or devices (with the aid of additional information), generally speaking, they are not an effective method to launch a broad attack.

The Commission also seeks information about alternatives to the CSRIC Report's recommendations that could be more effective.[40] Undoubtedly, the CRSIC Report's recommendations and the GSMA best practices are important, but they are not the only measures that carriers use to promote network security. In addition, next generation networks are being built and it is important to be constantly looking ahead to the next technology and anticipating the next set of potential vulnerabilities.[41] A new protocol, Diameter, is expected to replace many SS7 network functions and will be a critical component of 5G networks.[42] Carriers are leveraging the CSRIC Report's SS7 recommendations along with GSMA best practices and

[39] Testimony of Dr. Charles Clancy, Director and Professor, Hume Center for National Security and Technology, Virginia Tech, Before the House Subcommittee on Communications and Technology, Committee on Energy and Commerce on *Promoting Security in Wireless Technology*, at 60 (June 13, 2017) (Preliminary Transcript) https://docs.house.gov/meetings/IF/IF16/20170613/106104/HHRG-115-IF16-Transcript-20170613.pdf.

[40] PN at 2.

[41] *See, e.g.*, T-Mobile Sen Wyden Letter at 2 ("Innovation enables us to design security in new ways that will increase security while reducing the significance of SS7. This investment in the future of 5G is vital to enhance security and maintain U.S. leadership in the global wireless marketplace.").

[42] *See* CSRIC VI: Working Group 3, Network Reliability and Security Risk Reduction, Final Report – Recommendations to Mitigate Security Risks for Diameter Networks (2018) https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council (discussing how the industry can use the successful "playbook" it employed to combat SS7 threats to protect Diameter).

standards work elsewhere in the development of the Diameter protocol to reduce the risk of possible vulnerabilities. As the CSRIC Report noted, "[f]urther study needs to be considered for both Diameter and 5G security as these systems and networks are deployed."[43] Carriers and other ecosystem participants will be valuable partners with government and standards bodies in that work. U.S. government support and involvement in global standards processes is particularly important as companies and nation states jockey for influence over next generation networks.

V. INTERNAL INFORMATION-SHARING, PRIVACY PROTECTION, AND RECORD KEEPING, RAISED IN THE PUBLIC NOTICE, ARE BEING ADDRESSED BY INDUSTRY.

In its final set of questions, the Commission asks about "other considerations" including sharing of potential SS7 risks with carriers' internal business units and key business clients, protection of the privacy of subscriber data, and retention of network logs.[44] Carriers have taken these considerations into account.

Communications service providers strive to appropriately educate their internal teams and partners on evolving threats and responses. Carriers' teams have long been aware of SS7 issues and have been aggressively addressing them.[45] In addition, roaming agreements with peer providers are subject to rigorous security approaches, although international peering agreements

[43] CSRIC Report at 13.

[44] PN at 2.

[45] *See, e.g.*, T-Mobile Sen. Wyden Letter at 2 ("T-Mobile is aware of SS7 security issues and is addressing them with best practices and collaboration."); Sprint Sen. Wyden Letter at 1 ("Sprint has implemented multiple layers of security to protect its network, including its SS7 network, from malicious activity."); Verizon Sen. Wyden Letter at 1 ("Verizon is comprehensively addressing SS7 security issues"); AT&T Sen. Wyden Letter at 1-2 ("We have been actively assessing and responding to known SS7 threats for some time . . . . AT&T has employed an aggressive multifaceted approach to the SS7 threat.").

present more complexity. Overall, stakeholders throughout the global wireless ecosystem are aware of SS7 risks and corresponding mitigations. For example, for high value government employees or executives, additional tools are available. Carriers and the industry have been working with government to identify measures the enterprise network provider can take to manage and secure mobility.

Carriers also have implemented various measures to help protect the privacy of subscriber data from SS7 risks and other exploits. Carriers take the privacy of customer information seriously and undertake daily efforts to mitigate threats to privacy; they have robust privacy and data security programs and secure their users' information.[46] In addition, carriers support the use of end user device- or application-based encryption.[47] CTIA has long urged consumers and others to consider encryption and other defenses against cyberattacks,[48] and third-

[46] *See e.g.* AT&T, Privacy Policy (http://about.att.com/sites/privacy_policy), Verizon, Privacy Policy (http://www.verizon.com/about/privacy/privacy-policy-summary); T-Mobile, Privacy Policy (https://www.t-mobile.com/company/website/privacypolicy.aspx); and Sprint, Privacy Policy (https://www.sprint.com/en/legal/sprint-corporation-privacy-policy.html).

[47] *See generally* Verizon, *Voice Cypher*, http://www.verizonenterprise.com/products/mobility/enterprise-mobility-management-security/voice-cypher/ (last accessed May 2, 2018) ("The best security measures are invisible, easy to deploy and offer multiple layers of protection. Voice Cypher Ultra is a downloadable mobile app . . .. It's simple, hardware-free voice and messaging technology that works across multiple wireless carriers (or WiFi) to provide end-to-end encryption"). *See also* BlackBerry, David Kleidermacher, *How to Protect Yourself from SS7 and Other Cellular Network Vulnerabilities*, (Apr. 21, 2016), http://blogs.blackberry.com/2016/04/how-to-protect-yourself-from-ss7-and-other-cellular-network-vulnerabilities/ ("But there are simple actions you can take to protect the privacy of your sensitive data – phone calls, text messages, e-mails, etc. – that you transmit over mobile networks using mobile devices. The simple rule of thumb: always encrypt your data before it hits the wireless network."); *id.* (BlackBerry provides end-to-end encryption of the communications channel as well as S/MIME and PGP message encryption"); *id.* ("[U]se encrypted voice-over-IP").

[48] *See, e.g.*, CTIA, Consumer Resources, Protecting Your Data, https://www.ctia.org/consumer-resources/protecting-your-data (last accessed May 2, 2018) ("Use additional layers of security—like Virtual Private Networks (VPNs) and encryption applications—to further protect your sensitive information, especially on open networks"). CTIA recently lauded a CSRIC report that addressed "the effectiveness of shared efforts and the

party sources also echo this point.[49] The overall goal is to educate consumers and enterprise managers of their options for protecting sensitive data.

The Commission also seeks information about retention of network logs.[50] Carriers receive tens of billions of SS7 communications daily, so each organization must determine for itself what sort of logs and records make sense to retain and for how long. This is true for service providers and all others addressing cybersecurity. Carriers handle their network logs in an appropriate manner to support risk-based decisions, and there is no evident need for longer log retention or other regulatory steps on SS7 or other specific security concerns. Carriers respond to and anticipate security challenges by developing practices that meet the needs of their particular organizations, partners, and customers.

VI. CONCLUSION

The wireless industry has been executing against all the CSRIC Report's recommendations regarding SS7 network risks as part of its comprehensive approach to protect the networks. The industry remains vigilant and ready to adapt to the latest threats, treating SS7 as one of many ongoing and dynamic risks. The industry values its close collaboration with the federal government to address these and other concerns. Going forward, the Commission should

existing wealth of security tools currently in place for consumers, including encryption technologies." John Marinho, CTIA Blog, Report Recognizes Wireless Efforts to Protect Against Cyber Threats, http://www.ctia.org/news/report-recognizes-wireless-efforts-to-protect-against-cyber-threats (Apr. 5, 2018).

[49] *See* Samuel Gibbs, *SS7 hack explained: what can you do about it?*, Guardian (Apr. 19, 2016), https://www.theguardian.com/technology/2016/apr/19/ss7-hack-explained-mobile-phone-vulnerability-snooping-texts-calls (advocating for the use of encrypted messaging services to avoid the SMS network).

[50] PN at 2.

continue to facilitate collaboration between the wireless industry and government stakeholders, particularly through DHS and its existing channels for improved information sharing.

Respectfully submitted,

By: *<u>/s/ Melanie K. Tiano</u>*
Melanie K. Tiano
Director, Cybersecurity and Privacy

Thomas C. Power
Senior Vice President, General Counsel

Scott K. Bergmann
Senior Vice President, Regulatory Affairs

Thomas K. Sawanobori
Senior Vice President, Chief Technology Officer

CTIA
1400 Sixteenth Street, NW, Suite 600
Washington, DC 20036
(202) 736-3200

May 3, 2018