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 AT&T SERVICES, INC.

Pursuant to the Commission's Public Notice in the above-captioned proceeding,[1] AT&T Services, Inc. ("AT&T") submits these comments on implementation of Signaling System 7 ("SS7") security best practices. AT&T takes any threat to its network and its customers' communications seriously. AT&T has been actively assessing and responding to known SS7 threats for some time, and just as these threats can evolve over time, so do our means to identify and mitigate them.

SS7 is a signaling protocol that allows carriers to communicate with each other to deliver calls and text messages between their networks. Over the last half-century, SS7 has been integral to the explosion of telecommunications competition and advanced technology. Among other things, SS7 makes it possible for wireless customers to roam globally, spurring

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

the rapid growth of wireless technology around the world. It also supports enhanced features, such as call forwarding and caller ID, all to the benefit of consumers.

This expanded use of SS7 offers great benefits, but also presents evolving risk. Unlike cybersecurity threats from hackers, the growing number of carriers having *legitimate* credentials into the network creates the threat to SS7. At its inception, in the 1970s, roughly 10 trusted carriers worldwide had access to the SS7 network. With the explosion of competition, international calling and roaming, hundreds of carriers now have access to SS7, many of them in unstable or unfriendly nations where credentials can be compromised—or even sold on the open market. AT&T has therefore hardened and tuned its defenses to account for these developments given that the trust model is no longer fully reliable.

Moreover, given the importance of the SS7 system to global communications and interconnection between networks, any carrier response to an SS7 vulnerability must be mindful of the legitimate uses of SS7. Prior to implementation of any defense, a carrier must carefully research how its actions might impact its network. AT&T alone handles tens of billions of SS7 messages per day. And the vast majority of SS7 messages are legitimate, enabling consumers to complete critical communications. As the Communications Security, Reliability and Interoperability Council (CSRIC) SS7 working group concluded, "because the overwhelming amount of SS7 traffic is legitimate, carriers need to be measured as they implement solutions to avoid collateral network impacts."[2]

[2] *FCC CSRIC Working Group 10 Final Report: Legacy Systems Risk Reductions* (March 2017), at 11, available at https://www.fcc.gov/files/csric5-wg10-finalreport031517pdf

Against this backdrop, AT&T has employed an aggressive, multifaceted approach to the SS7 threat. Public disclosure of the specific technology we have deployed to meet any cybersecurity threat (and where we stand in implementing those defenses) would only provide bad actors a blueprint for how to evolve their techniques and defeat our defenses. Nonetheless, we can confirm that AT&T has taken significant, aggressive steps to protect the SS7 network. For example:

- AT&T has implemented extensive blocking and filtering of nefarious SS7 messages, including blocking of the vulnerabilities identified by researchers, industry groups and our own testing. AT&T has also implemented "SMS Home Routing."

- AT&T has, alone and in concert with our vendors, implemented new firewalls and other innovative technologies to monitor, inspect, and filter nefarious traffic.

- AT&T has deployed hardware and software necessary to implement the GSM Association (GSMA) best practices on protecting SS7. We have cautiously deployed advanced filtering recommended by GSMA because those filters may raise heightened concerns of blocking legitimate traffic.

- AT&T has tested its network and worked with outside experts to better understand and assess the threat to SS7, as we routinely do with network security threats. We have responded to issues identified in such testing and will continue to do so as threats evolve. Our testing has shown that our aggressive steps to meet the threat are working.

- We have collaborated with the FCC, the Department of Homeland Security (DHS), the intelligence community, and the industry to share information concerning potential threats and our responses.

This last point above concerning our work with the FCC and DHS merits emphasis. Among other things, we participated with DHS on the FCC's nine-month-long CSRIC working group to study the SS7 risk and provide recommendations on how to best mitigate the threat. In December 2016, the working group, with DHS's participation, prepared a risk assessment that included information about SS7 attacks bad actors may utilize. The working group deemed this information so sensitive that it was redacted from the final report pursuant to a

non-disclosure agreement. In March 2017, the working group released a public report with recommendations for best practices to reduce SS7 security risks.[3] Together, the wireless industry publicly committed to implementing these recommendations.[4] We also participated in the follow-on CSRIC Working Group 3, which studied similar vulnerabilities to the Diameter signaling system utilized by 4G/LTE networks. That working group concluded that the "industry can use the successful 'playbook' it employed to combat SS7 threat to protect Diameter."[5] AT&T has already turned its attention to Diameter.

Moreover, AT&T's engagement with the FCC and DHS on SS7 goes well beyond the CSRIC working groups. We have had ongoing meetings with DHS concerning the SS7 threat before, during and after the working group's existence. We have met with the FCC and DHS both as an industry (through CTIA) and individually. In these meetings, we have shared specific, confidential information concerning our knowledge of known SS7 threats and the specific actions AT&T is taking (and plans to take) to address those threats, including the filtering techniques and other technical capabilities we have placed into our network. AT&T has also updated the agencies as we have implemented the GSMA best practices.

---

[3] *Id.*

[4] *CTIA Statement: SS7 and FCC CSRIC Recommendations*, available at https://www.ctia.org/docs/default-source/default-document-library/ss7-statement-2017-final.pdf.

[5] *FCC CSRIC Working Group 3 Final Report: Recommendations to Mitigate Security Risks for Diameter Networks* (Mar. 14, 2018), at 5 available at https://www.fcc.gov/files/csric6wg3finalreport32018pdf

CONCLUSION

AT&T shares the Commission's interest in protecting the SS7 network from malicious actors and stands ready to work cooperatively, including providing more detailed information in an appropriate, confidential manner.

Respectfully submitted,

/s/ Christi Shewman

Christi Shewman
Gary Phillips
David Lawson
AT&T Services, Inc.
1120 20th Street, N.W.
Suite 1000
Washington, D.C. 20036
(202) 457-3090

May 3, 2018

Attorneys for AT&T Services, Inc.