CTIA Statement
SS7 and FCC CSRIC Recommendations

The wireless industry maintains security as a top industry priority and responds rapidly to mitigate possible threats. The U.S. wireless industry's response to possible Signaling System 7 (SS7) threats demonstrates the industry's commitment to the security of its networks and its customers' communications.

At a basic level, the SS7 network allows carriers to communicate with each other in a common language to complete communications. The network is particularly important to allow customers to roam seamlessly between carriers, both domestically and internationally. The SS7 network was designed decades ago as a carrier-only network where trusted carriers carefully safeguarded their credentials to access the network. And for decades, the "carrier trust model" worked because the few global and national carriers carefully safeguarded access to SS7. Problems have arisen in connection with expanding SS7 access to a large number of carriers and locations where credentials can be compromised, as highlighted in various media reports. [1] As a result, industry took an aggressive but measured approach, as it implemented steps and solutions to avoid collateral network impacts to subscribers and risk blocking legitimate traffic. Companies must dynamically balance the risk of dropping legitimate communications against the security risks associated with malicious abuse of legitimate credentials, and no one size fits all solution will work for all carriers and platforms.

While the overwhelming majority of communications on the SS7 network are legitimate, the industry has been engaged on possible SS7 security issues. For instance, to complement and advance individual company efforts, the international carrier association GSMA issued security best practices and guidelines to secure signaling interconnection and maintain continued advancements in information sharing of threat intelligence to adapt monitoring, filtering and data analytics.[2] In addition, GSMA has recommended controls to address emerging security risks for 5G.[3] In addition, industry worked with the Federal Communications Commission (FCC) and the Department of Homeland Security (DHS) as part of the Communications Security, Reliability and Interoperability Council (CSRIC)[4] Working Group established to address SS7 threats and related topics in June 2016.

In the CSRIC, industry subject matter experts, working with the FCC and DHS, assessed different attack vectors identified in a variety of settings, including blogs, conferences, and standards meetings, as well as industry and government forums. The effort considered reported vulnerabilities (e.g., those discovered by industry or security researchers) and disclosed exploitation of vulnerabilities. It also documented Industry actions that have been taken to mitigate the vulnerabilities and additional actions

[1] 60 Minutes, *Hacking Your Phone* (Apr. 17, 2016) http://www.cbsnews.com/news/60-minutes-hacking-your-phone/.

[2] *See* GSMA, Fraud and Security Group https://www.gsma.com/aboutus/leadership/committees-and-groups/working-groups/fraud-security-group.

[3] *See* GSMA, *The 5G era: Age of boundless connectivity and intelligent automation* (2017) https://www.gsmaintelligence.com/research/?file=0efdd9e7b6eb1c4ad9aa5d4c0c971e62&download.

[4] FCC, Communications Security, Reliability and Interoperability Council (CSRIC).

recommended, while being cognizant that the overwhelming amount of SS7 traffic is legitimate.

The FCC CSRIC effort is memorialized in a Final Report issued in March 2017,[5] which captures the SS7 situation, potential targets, prominent attack methodologies and their potential impacts, as well as key best practices and countermeasures to mitigate threats.

CTIA and its members have embraced and support the CSRIC Final Report recommendations:

1. continued signaling interconnection monitoring and filtering as outlined in the Risk Assessment report;
2. continued use of GSMA security best practices and guidelines to secure signaling interconnection and maintain continued advancements in information sharing of threat intelligence to adapt monitoring, filtering and data analytics;
3. engage signaling aggregators in their efforts to address overall security;
4. leverage and expand existing threat information sharing resources with the DHS National Coordinating Center for Communications (NCC), the Communications ISAC and collaboration with law enforcement;
5. ongoing security assessment of network signaling infrastructure to detect and mitigate possible threat vectors, based on best practices and standards;
6. encourage the use of available encryption technologies, for both voice and data communications for highly sensitive and critical applications or for VIPs that may often be targeted by bad-actors;
7. continued automated threat information sharing through the CTIA sponsored information sharing Pilot to advance telecommunications specific use-cases; and
8. use of GSMA recommended controls to address emerging security risks for 5G.

The CTIA cybersecurity working group supports both the CSRIC and GSMA recommendations and the broader mobile industry is in the process of implementing these solutions. This technology is vital and continues to empower expansion of mobile technologies, competition, and global interoperability. These global opportunities, however, come with global threats that impact all of the carriers that connect to the network. The U.S. carrier industry stands committed to leading efforts to innovate and enhance the security of SS7.

[5] FCC, Communications Security, Reliability and Interoperability Council, WORKING GROUP 10: *Legacy Systems Risk Reductions Final Report* (Mar. 2017) https://www.fcc.gov/file/12153/download.