COMMITTEE ON
SCIENCE, SPACE, & TECHNOLOGY
Lamar Smith, Chairman

For Immediate Release
June 27, 2018

Media Contacts: Heather Vaughan, Bridget Dunn
(202) 225-6371

Statement by Chairman Ralph Abraham (R-La.)

Bolstering Data Privacy and Mobile Security: An Assessment of IMSI Catcher Threats

Chairman Abraham: Good afternoon and welcome to today's Oversight Subcommittee hearing: "*Bolstering Data Privacy and Mobile Security: An Assessment of IMSI Catcher Threats.*" The purpose of today's hearing is to examine the threats that IMSI catchers and other similar technologies pose to mobile security and user privacy.

IMSI catchers and rogue base stations—commonly known by their brand name "Stingray"—are devices used for intercepting cellular traffic and data. Today we will hear from government and academic experts about the basics of this technology, the ways in which it can be used by both legitimate and illegal actors, and potential methods to mitigate the risks these devices pose.

Regrettably, although they were invited, the Department of Homeland Security (DHS) declined to provide a witness today and instead provided a briefing to members and staff last week. While this was helpful in giving some context to this matter, it was no substitute for a public discussion on such a serious issue. It would have been substantially more helpful for DHS to have been present today, to be part of this dialogue, inform the American public, and answer questions about their work in this area. With that said, I would like to thank our witnesses for participating today and taking time out of their schedules to testify on this important matter.

Historically, the use of IMSI catcher technology has been limited to law enforcement, defense and intelligence services. This was due in large part the high cost of acquiring the equipment. However, as sophisticated technologies have become more commonplace and advances in manufacturing have made the production of highly technical products easier and cheaper, IMSI catcher technology and nefarious actors looking to exploit it have proliferated.

While awareness is important, it is simply not enough to acknowledge an issue needs to be addressed. Instead, we must also gain an understanding of the technological nature and complexity of disruptive technologies like IMSI catchers to alleviate the challenges they present. This is a responsibility the committee takes seriously, and one which the committee has a long history of meeting through vigorous oversight of emerging forms of research and technology. I believe today's hearing will add yet another important chapter to that history.

As with much of technology in the modern age, IMSI catchers are a double-edged sword. On the one hand, when used for legitimate law enforcement purposes, these technologies have the potential to positively impact society in a substantive and meaningful way. The

ability to covertly track a suspect or intercept their data has the potential to help law enforcement coordinate safer arrests and put more criminals behind bars, keeping our men and women in uniform, as well as our communities, safe.

However, as we have seen with many new technologies and law enforcement tools, striking the appropriate balance between safety and privacy is not always easy. Just this past week, the Supreme Court ruled in *Carpenter v. United States* that cell phone location records are protected under the Fourth Amendment, previously a legal grey area. While this ruling does not purport to apply to real-time data tracking—the type IMSI catcher technology could provide—it raises the question of what the appropriate balance is between protecting privacy and empowering law enforcement to do their job.

Similarly, we must consider what defenses we can and should employ to protect our privacy and national security. IMSI catcher technology is ripe for exploitation by foreign nations seeking to spy on American government officials and is likely already being used to do so. The cryptographic standards and methods used to protect US government officials and important government information are something the National Institute of Standards and Technology is well positioned to produce, but this too creates a dilemma.

As we saw with the San Bernardino terrorist's iPhone, sophisticated encryption meant to protect user data and privacy brings with it a set of different, but no less consequential, issues. In the case of IMSI catcher technologies, to what degree should the general public be able to shield themselves from being caught in a foreign intelligence operation? To what degree might techniques meant to shield data from prying eyes prevent law enforcement from doing their jobs? How much privacy should we trade for security at the civilian and governmental levels? These are fundamental questions that must be asked.

While I doubt we will hear an easy answer to these questions during today's hearing, we will hear informed perspectives from our witnesses on these and other important questions. It is my hope that we will leave here not only with a better understanding of this technology, but with forward-looking thoughts about possible answers to, and solutions for, these tough questions. Again, I want to thank our witnesses for agreeing to be here to highlight this important topic.

###