OPENING STATEMENT

Ranking Member Eddie Bernice Johnson (D-TX)

House Committee on Science, Space, and Technology
Subcommittee on Oversight
"Bolstering Data Privacy and Mobile Security: An Assessment of IMSI Catcher Threats."
June 27, 2018

Thank you Chairman Abraham.

Cell-site simulators, also known as Stingrays, or IMSI catchers, is a technology that can be used to locate cellular devices and possibly intercept voice calls, text messages, and data communications from the cellular device. It is a valuable tool for our law enforcement and intelligence communities.

It is also, undoubtedly, a technology used by foreign intelligence services operating here in the United States. Indeed, the genesis of today's hearing were recent press reports that a Department of Homeland Security (DHS) pilot program found rogue cell sites throughout Washington, D.C., including near the White House, FBI headquarters, and the Pentagon.

It is clear that foreign intelligence agencies are seeking to use cell site simulators to collect intelligence on federal officials. What are we as a government doing to counter this particular threat? Unfortunately, neither the Department of Homeland Security (DHS) nor the Federal Bureau of Investigation (FBI) is here today to help provide some answers to that question.

It is also unfortunate, as my colleague Mr. Beyer has pointed out, that President Trump appears to be taking no safeguards to protect himself from these cyber threats, and the Science Committee has taken no steps to use our oversight authority to investigate the White House's lack of cybersecurity precautions that we expect all other federal agencies to follow. I reiterate Mr. Beyer's call and request that we hold a hearing on this subject in the near future.

I am glad though to have our witness panel here today, who can provide us with advice on what Congress should be doing to protect federal officials and federal agencies from cell site simulators that exploit our cybersecurity vulnerabilities, particularly those that impact our national security interests.

Cell-site simulator technology also has implications for the privacy of Americans, as a law enforcement operation utilizing a cell site simulator could be gathering data from thousands of nearby innocent citizens. In Baltimore, for instance, police used this technology without obtaining a warrant thousands of times in violation of the Fourth Amendment to the U.S. Constitution regarding an unreasonable search. Last week, the U.S. Supreme Court weighed in on this issue requiring police to obtain a warrant to gather cell phone location data. However, their decision did not specifically apply to cell site simulators. So, it is unclear how these key privacy issues will be addressed by law enforcement agencies in the future.

I am glad Dr. Jonathan Mayer from Princeton University—a lawyer and a computer scientist — is here today. He is uniquely qualified to speak on these important privacy issues, as well as the wider implications of this technology and the dangers it poses to our national security and our privacy. I look forward to hearing from him and our other witnesses about how we can protect our national security and the privacy of our citizenry from attack by these rogue cell sites and other cyber-threats that can target our mobile devices.

Thank you Chairman Abraham and thank you to all of our witnesses for being here today

I yield back.