OPENING STATEMENT

Ranking Member Don Beyer (D-VA)
of the Subcommittee on Oversight

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 or IMSI catchers, pose risks to both our national security and our personal privacy. These devices are about the size of a laptop computer and can be placed in a van, hotel room, drone aircraft, or operated by someone sitting on a park bench. These rouge cell stations masquerade as legitimate cell towers and gather the data of cell phones in their proximity. They are powerful tools employed by both friendly and hostile intelligence agencies, criminals and others. They also play an important role in the operations of U.S. law enforcement and the U.S. intelligence community. However, U.S. law enforcement agencies have not always obtained appropriate authorization from the courts before they have employed these tools against suspected criminals. This has led to improper incursions into the private lives of hundreds of American citizens.

Last week, the Supreme Court ruled that the government must now obtain a warrant when collecting cell phone data in certain cases. The court found, and I quote – "A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales. Accordingly, when the Government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user," unquote. However, the court added that it was a narrow ruling, specifically stating, "We do not express a view on matters not before us: real-time CSLI [Cell-Site Location Information] or 'tower dumps." Unfortunately, it seems the constitutionality of cell site simulator use by law enforcement agencies without a warrant remains unsettled.

Rogue cell site simulators have not only affected our privacy, but they have endangered our national security. Last year, a Department of Homeland Security (DHS) pilot project identified several rogue cell site simulators near the White House and Pentagon—raising the specter of foreign intelligence agencies using IMSI catchers to target senior U.S. government officials here in our Nation's Capital.

Ironically, at the same time, we are holding an oversight hearing on the threat to mobile security of these sorts of rogue cell sites, President Trump continues to ignore basic cybersecurity practices. This has created a threat not just to his own personal privacy but also to our national security. A headline from a *CNN* story in April read, **"Trump ramps up personal cell phone use."** In May, *POLITICO* summed up the President's attitude towards the cybersecurity issues we are discussing today and the security precautions that should be taken to counter these threats.

The headline read: ***"'Too inconvenient': Trump goes rogue on phone security.'"*** Making matters worse, President Trump recently said that he provided his direct phone number to North Korean dictator Kim Jong-un. Doing this has opened up an additional threat known as a Signaling System Seven or SS7 attack that may permit access to President Trump's personal cell phone remotely by North Korean intelligence operatives. Earlier this month, *WIRED* magazine published a story with the headline: ***"Trump Says He Gave Kim Jong Un His Direct Number. Never Do That."***

I am attaching all three articles to my statement.

Ongoing use of a reportedly unsecure cell phone by the President of the United States raises serious cybersecurity issues that this Committee should be examining. The Majority's Oversight Plan for the 115th Congress said the Science Committee would investigate cybersecurity incidents and compliance with "federal information security standards and guidelines" *"regardless of where they may be found."* Let me repeat, quote: *"regardless of where they may be found."* I wrote to Chairman Smith with Ranking Member Johnson and Mr. Lipinski in February 2017 pointing out numerous cybersecurity practices of serious concern at the White House that warranted investigation. Unfortunately, we have seen no efforts by this Committee to uphold its oversight responsibilities to the American public and investigate these issues.

Chairman Abraham, holding this hearing and investigating the potential threat posed by rogue cell site simulators is a good idea. But I don't understand how we can investigate these issues and the specific threats that have been identified within blocks of the White House while ignoring the White House and President Trump's own failure to abide by cybersecurity best practices. In January 2018, the White House Chief of Staff banned the use of personal cell phone use in the West Wing by White House employees. Yet, multiple media stories have continued to report that the President refuses to give up his personal cell phone or take proper cybersecurity measures to help identify and diminish cybersecurity threats. The President should not be held to a different standard than the rest of the federal government and our Committee should help ensure the Executive Branch is taking appropriate cybersecurity measures to protect Mr. Trump from foreign adversaries, even if the President himself won't.

I look forward to hearing from all of our witnesses today who can help us explore ways to enhance our cybersecurity tools and plug our cybersecurity weaknesses. It is unfortunate that we do not have witnesses representing the Department of Homeland Security (DHS) or the telecommunications industry. I hope we are able to hear from them in the future. Successfully addressing these issues will take a collective effort and a continued commitment from a wide-range of stakeholders.

Thank you, Chairman Abraham. I yield back.