Statement of Subcommittee Chairman John Ratcliffe (R-TX)
Cybersecurity and Infrastructure Protection Subcommittee

"Understanding the Cybersecurity of America's Aviation Sector"

September 6, 2018

Remarks as Prepared

I am glad to be holding this hearing with my good friend, and Chairman of the Transportation and Protective Security Subcommittee, John Katko. I want to thank him for convening this hearing with me today to examine this topic that fits hand in glove with the security of our nation.

I have always said that cybersecurity is national security. And there is no better example of that than in the aviation industry.

When we think of threats broadly to the industry, traditional avenues of attack are what first come to mind. These threats, such as hijackings and bombings, will continue to pose a major security concern moving forward. However, as devices, aircraft, and systems become more interconnected, cybersecurity will increasingly play a larger role in aviation security.

Because nation states, cyber criminals, and "hacktivists," all possess an incentive to manipulate systems within the sector.

Whether it be looking to gain a competitive advantage, a financially motivated action, or simply a political statement, the space will always be crowded by malicious actors seeking to do harm.

This is why we need to understand all avenues of attack, to prioritize their severity, and mitigate those vulnerabilities as quickly as we can.

Innovation has brought increased efficiencies to daily life, however, it has also tied together networks like we have never seen before. Therefore, this is not a single-minded task. We cannot be narrow in our focus, as we must explore the entire aviation ecosystem as a whole.

We cannot have a single weak link across the entire chain, or else it could all fail.

For example: A ransomware attack which targeted the city of Atlanta earlier this year forced Hartsfield–Jackson Atlanta International Airport to turn off its Wi-Fi services for hours.
This is one of many examples illustrating the cross-cutting nature of the sector. All which pose inherent logistical, financial, and security concerns.

Therefore, it becomes incumbent upon the Department of Homeland Security, Congress, and the private sector to work together to find ways to create resilient systems. To create redundancies. To share threat information. And to build safety and trust into systems that have become integral to American travel.

Trust is instrumental in the continued health of the aviation industry. Customers and travelers need to have faith in the systems they are using, whether that be arrival boards or the airplanes themselves. Losing the trust of the everyday American would be disastrous for the sector and gaining it back would be an uphill battle as we cannot explicitly see increased firewall protection for example.

Furthermore, safety really is key as well. The aviation industry rises above all others in this case, as safety has been culturally built into the sector over time. The lessons learned from 9/11 have matured both private sector and federal government entities to the point that they are at today. However, we need to clearly delineate rolls of such entities as NPPD, TSA, and the FAA which we have come to rely on for our security concerns.

We must build partnerships both within the private sector and within government. Partnerships such as the Aviation Cyber Initiative, which brings together government stakeholders from DHS, DOT, and DOD to tackle cybersecurity problems across the aviation sector. It provides auditing on a voluntary basis to furtherer the goal of a safer, more secure ecosystem. DHS's National Protection and Programs Directorate recently announced the creation of a National Risk Management Center, in its effort to enhance risk management integration across the public and private sectors. I am very interested in the rollout of this Center and hope that it will become another essential tool for public private collaboration focused on cybersecurity.

By leveraging existing practices and partnerships already in existence, the aviation industry can maximize security benefits. A 2016 study by SITA found that 91 percent of airlines are planning to invest in cyber programs over the next 3 years, up from only 41 percent in 2013. Stakeholders remain poised to tackle the issues at hand and ensure a safe cyber ecosystem within their sector, and it is my hope that organizations like DHS's NPPD are offering support that is beneficial to this sector.

In our continued efforts to support the work and mission space of NPPD, I want to remind my colleagues that late last year, the House passed H.R. 3359, the Cybersecurity and Infrastructure Security Agency Act, a bill that is essential to solidifying and strengthening DHS's cybersecurity mission and would also support NPPD's efforts to bolster aviation cybersecurity.

I am excited to explore the issue of aviation cybersecurity today. I have faith that all parties will rise to the occasion and ensure that the American people can always have trust in the cybersecurity of the aviation sector.

I want to thank the witnesses for their time and I look forward to their testimony.

###