Statement of Ranking Member Cedric Richmond

Cybersecurity and Infrastructure Protection Subcommittee Hearing

UNDERSTANDING CYBERSECURITY THREATS TO AMERICA'S AVIATION SECTOR

September 6, 2018

Seventeen years ago, 19 terrorists weaponized 4 passenger airplanes and launched the most devastating attack on U.S. soil since Pearl Harbor. As we struggled to understand how such a horrific tragedy could happen, the Chairman of the 9/11 Commission issued a painful indictment: "This was a failure of policy, management, capability and above all, *a failure of imagination.*"

Since then, we have invested heavily in securing airplanes and airports against the kinds of attacks perpetrated by the 9/11 terrorists. But the threat landscape has evolved, and our adversaries have changed. Those who wish to do us harm have new tools at their disposal – giving them the ability to target aviation systems without stepping foot in an airport and without clear lines of attribution.

In March, the Department of Homeland Security and the FBI issued a joint alert warning that Russian government cyber activity had been targeting U.S. critical infrastructure, including the aviation sector. And research conducted by the DHS' Science and Technology Directorate have revealed troubling vulnerabilities in aircraft systems.

Although I am encouraged by Federal efforts to build awareness and address cybersecurity vulnerabilities to aviation infrastructure, I am concerned that we are, once again, playing catch up with our adversaries.

As we speak, the Transportation Security Administration does not require airport security plans to address cybersecurity vulnerabilities. And it is unclear how cybersecurity factors into safety considerations involved in building aircraft. We must do better.

This hearing is an important step in our efforts to understand the full scope of cyber vulnerabilities to aviation assets and to help relevant Federal agencies work with stakeholders to manage and mitigate cyber risks. Pursuant to the National Aviation Security Strategy, an interagency taskforce – known as the Aviation Cyber Initiative – is charged with reducing cybersecurity risks to the Nation's Aviation Ecosystem.

The ACI is co-chaired by the Department of Homeland Security, the Department of Defense, and the Department of Transportation, and its charter is being updated to facilitate the tri-chair structure. I will be interested in hearing from our witnesses today about ACI's outreach to the stakeholder community and about the nature of aviation asset owners and operators' engagement with the ACI.

More generally, I will be interested to learn how effectively the Federal government shares cyber threat information across the aviation sector, and how that information informs efforts to harden assets, secure networks, and train aviation workers – from pilots and flight attendants to airport employees.

Finally, I will be interested in learning about the other challenges associated to improving the cybersecurity posture of the aviation industry – from technology to resources.