FOR IMMEDIATE RELEASE

Statement of Ranking Member Bennie G. Thompson (D-MS)

Understanding Cybersecurity Threats to America's Aviation Sector

Subcommittee on Cybersecurity & Infrastructure Protection and Subcommittee on Transportation & Protective Security Joint Hearing

September 6, 2018

Next week, we will observe the anniversary of the terrorist attacks of September 11, 2001.

Seventeen years ago, our adversaries exploited the cracks in our aviation security apparatus to carry out the deadliest terrorist attack in our nation's history.

Since that time, we have focused on closing those gaps, making improvements to the way we share threat intelligence, screen passengers, and secure physical aviation infrastructure.

Although I recognize the progress we have made improving aviation security, I am concerned that we are overlooking an important attack vector: cyber.

The aviation sector represents a wide array of critical assets, including the systems and networks that support airports, air traffic control, and aircraft, to name a few.

We rely on these diverse assets to support not only personal travel, but also commercial shipping, disaster relief, and a host of other activities essential to the health of our economy and national security.

All these assets are subject to a unique set of cybersecurity risks and vulnerabilities.

But we have done little to protect them against evolving cyber threats.

When it comes to physical security at our airports and our airplanes, we impose strict requirements designed to keep bad actors, explosives, and other illicit materials out.

But there are no equivalent cybersecurity standards.

Although we encourage owners and operators of aviation assets to take advantage of DHS cybersecurity programs and services, it is no substitute for requiring cybersecurity measures as part of site security plans.

And in many cases, aviation sector owners and operators struggle with the same cyber challenges that plague other industries: a national shortage of skilled cybersecurity personnel, a workforce with minimal cybersecurity training and awareness, and resource constraints across the board.

These gaps in our security framework represent “low-hanging fruit” for our adversaries.

A relatively simple intrusion could upend airport operations, costing airlines millions.

A more sophisticated breach of a cockpit could bring down a plane.

I am far from convinced that the Federal government is investing enough in research around aviation-related cyber vulnerabilities.

Right now, some of the most significant Federal research in this area is being led by the DHS Science and Technology Directorate, which operates on a shoestring budget that Republicans in Congress continue to slash, year after year.

Nevertheless, last year, officials involved in this research reportedly managed to carry out a remote hack of a commercial passenger jet.

These findings underscore that this threat is real, and more attention is needed.

I look forward to hearing from this panel of witnesses today, and I hope they will give us a candid assessment of the cybersecurity posture of our aviation sector.

I will be interested to hear what progress has been made on areas like cyber threat information sharing, and how Congress can support do to promote those efforts.

# # #

Media contact: Adam Comis at (202) 225-9978