Statement of Ranking Member Bonnie Watson Coleman

Subcommittee on Transportation and Protective Security Joint Hearing

"Understanding Cybersecurity Threats to America's Aviation Sector"

Thursday, September 6, 2018

I am really glad we are holding this hearing because it seems to me that the topic of aviation cybersecurity has not received the attention it demands. Threats to the transportation sector are constantly evolving, and efforts to secure transportation must go beyond simply reacting to the most recent attempted attacks.

Next week, we will commemorate the 17th anniversary of the September 11th attacks. One reason terrorists were able to carry out such deadly attacks on September 11th is that they took us by surprise. The U.S. aviation sector was vulnerable because security efforts had not focused on the possibility of terrorists hijacking a plane and using the plane itself as a missile.

In the years since then, we have invested heavily in aviation security by hardening cockpit doors, creating the TSA, improving passenger and baggage screening, and refining intelligence sharing and vetting processes. These efforts have unquestionably made air travel more secure, but we cannot let our guard down now.

We must urge security agencies to think creatively about potential new attack vectors, as terrorists continue to search for vulnerabilities to target.

With that in mind, we must do more when it comes to the cybersecurity of transportation systems. Seventeen years after terrorists gained access to cockpits via physical means, we cannot allow them to gain access to cockpits via cyber means.

Last fall, reports emerged that a research team led by the DHS Science and Technology Directorate was able to remotely hack into the systems of a commercial passenger jet. In the wrong hands, such a capability could result in mass casualties. Even a much less drastic security breach could have major consequences.

The aviation sector relies on a vast network of interconnected systems, including air traffic control, airports, airline operations systems, and reservation and ticketing systems. A cyber attack against any one of these systems could cause chaos and confusion, resulting in cancelled flights and diminished consumer confidence. Such an attack would likely cost airports and airlines millions and have lasting effects on the economy.

Despite the clear vulnerabilities and consequences of a cyber attack within the aviation sector, not much has been done to improve cybersecurity. Although TSA requires airports and airlines to adopt and implement security programs covering a wide range of measures to protect against attack, TSA does not require those programs to include any cybersecurity measures.

Instead, TSA only shares a list of recommended best practices for airports and airlines to implement at their discretion. When it comes to securing air travel, voluntary measures are not enough.

That is why I am working with my colleagues to develop legislation to require TSA to issue new rules for airports and airlines requiring implementation of baseline cybersecurity measures.

Additionally, while this hearing is focused on the aviation sector, I would be remiss if I did not note that these issues affect other modes of transportation as well. Mass transit, passenger rail, freight rail, and pipeline systems all rely on networks that must be secured against cyber attacks.

It is my hope that today's hearing will provide us with more information on current cybersecurity efforts within the aviation sector and on what work remains to be done.