PREPARED STATEMENT OF
CHRISTOPHER PORTER, CHIEF INTELLIGENCE STRATEGIST, FIREEYE, INC.,

BEFORE THE HOUSE HOMELAND SECURITY COMMITTEE
SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND SECURITY TECHNOLOGIES
SUBCOMMITTEE ON TRANSPORTATION AND PROTECTIVE SECURITY

Understanding Cybersecurity Threats to America's Aviation Sector

SEPTEMBER 6, 2018

Thank you Chairman Ratcliffe, Ranking Member Richmond, Chairman Katko, and Ranking Member Coleman for convening this joint hearing today. We appreciate the opportunity to share FireEye's perspective on threats to the aviation sector and provide an overview of how the private sector is helping to secure the sector.

My name is Christopher Porter, and I'm the Chief Intelligence Strategist for cybersecurity company FireEye and a Nonresident Senior Fellow at the Atlantic Council. At FireEye I manage our "Intelligence for Executives" program for senior corporate and government clients across the globe. Our strategic intelligence products reach more than 4,000 customers in 67 countries.

Prior to joining FireEye in 2016, I served for nearly nine years at the Central Intelligence Agency, including an assignment as the cyber threat intelligence briefer to White House National Security Council staff, several years in counterterrorism operations, and warzone service.

In addition to the 300-plus security professionals responding to computer intrusions, FireEye has over 200 cyber-threat analysts on staff in 18 countries, speaking 30 different languages, to help us predict threats and better understand the adversary – often by considering the political and cultural environment of the threat actors. We have an enormous catalog of threat intelligence, and it continues to grow everyday alongside the continually increasing attacks on organizations around the world.

FireEye is supporting the aviation sector here at home. We're protecting the Transportation Security Administration with both email and web inspection, managed by the Department of Homeland Security's Enterprise Security Operations Center. As TSA continues to stand up its intelligence capabilities, we are providing support through their subscription to our intelligence reporting.

The Federal Aviation Administration also makes great use of our intelligence reporting and they're using our malware analysis tool to help prevent and detect future cyber attacks.

I want to share with you today FireEye's perspective responding to breaches in the aviation sector and from the intelligence we have collected on what might be coming next.

I am sure it will come as no surprise to you that the aviation sector is one of the most targeted for cyberattack. Safe, reliable air transport is vital for everything from national defense to global commerce to personal freedom. Malicious actors seeking to undermine America's strength in aviation through cyberattacks and theft include foreign governments, terrorists, organized crime, and other non-state actors.

I want to start by discussing the most common cyber threat facing the aviation industry: cyberespionage. Foreign governments routinely seek to steal industrial secrets from manufacturers, researchers, designers, and operators of both military aircraft and cutting edge civilian planes. China, Russia, and more recently Iran have all targeted the U.S. or its close allies for theft of aviation secrets via computer network operations.

All three countries also routinely target ticketing and traveler data, shipping schedules and manifests, and partner industries such as railways and hotels as they gather counterintelligence data on suspicious travelers and intelligence on VIPs they wish to track.

There are two aspects of cyberespionage targeting the aviation sector overall that I want to emphasize: first, that because of its pervasive nature, the best defense against cyberespionage is rapid, detailed information sharing with context. Our company pushes alerts to customers in real-time, and industry groups share information between peers because, as we have learned, a threat to one is often a threat to all. The US Government also shares threat information, although it is generally classified and available only to cleared vendors; there is room for improvement in government information sharing with uncleared industry partners. Most importantly, the timeliness of information within industry and between the private sector and US Government must improve. In my line of work, if we can't provide context and additional information in 24-48 hours of an attack, we have not met customer expectations.

The second thing to know about cyberespionage though is that, because it is routine, it should not be viewed as destabilizing. Media reporting on cyber incidents is often focused on the worst-case scenario in ways that are sometimes unjustified and needlessly alarm the public or inflame opinion against a foreign adversary. Every major cyber power, including the United States, has an interest in knowing about the potential defense technology developments of both its friends and potential threats, and the US aviation sector is not unique in being targeted in this way.

When cyberespionage operators get a foothold on a system, they can often use that access for stealing information or to launch a disabling or destructive attack using the same technology. But they rarely choose to do so, and in the US there are significant redundancies in place to ensure safety. A crashed IT system does not mean a crashed plane, and it's important for the public to keep that in mind.

So while cyberespionage on its own does not pose an urgent threat to life, I am concerned that continued theft of trade secrets poses a long-term threat to American economic health.

Aviation is one of our nation's leading export industries, and China in particular is harnessing all aspects of national power to displace the U.S. as a military and economic power in Asia and worldwide. Chinese theft of U.S. intellectual property for commercial purposes has almost entirely dropped off since a September 2015 agreement between President Xi of China and President Obama, but because aviation research and development is so closely tied to national defense this particular sector of the American economy never stopped being targeted.

Chinese hackers pursue fewer targets in the United States than they did before the Xi-Obama Agreement, but they have just as many hackers who are more skilled and better resourced than ever, meaning that industries that do continue to be threatened face a greater threat than ever before that technologies the U.S. spends billions developing will be stolen and adopted by economic competitors and military rivals in China.

Cybercriminals likewise pose an economic threat to the aviation sector and its customers. For years we have seen airlines and third-party ticket sellers exploited so that illicit tickets could be resold for profit in underground fora. Because airlines are trusted by their customers with a wide variety of sensitive personal data, they are also frequently targeted by cybercriminals looking to gather data to enable other types of fraud. In the last two years, our devices have detected a sharp increase in the use of ransomware to temporarily disable airline ticketing and support operations—air travel is a time-sensitive business, and cybercriminals know that they can extort quick payment from airlines that are unable to move passengers until their systems are decrypted.

Finally, in addition to threats to the aviation sector's proprietary information, customer records, and systems that support flight operations, there are cyber threats intended to use aviation's prominent place in our lives as a means of creating psychological damage or political pressure. Airports in Europe, the Middle East, Southeast Asia, and here at home have had their websites defaced or disrupted, mostly by non-state actors seeking to draw attention to a particular political cause.

The primary victim in these situations are members of the public who may wrongly fear that a loved one is at risk or grow in their distrust of flying, even though the affected systems may be public-relations focused and support no flight operations at all. The fear these operations cause is particularly pronounced when those outages are caused by groups affiliated with terrorists.

In other cases, these virtual sit-ins that affect a company's website have, in limited cases, delayed takeoffs for airlines that also relied on those computers to make or distribute flight plans, though even these attacks did not have a direct effect on flight safety.

It is important that officials and airlines representatives communicating with the public during such events differentiate between taking down systems that cause inconvenience from those that directly support flight operations and passenger safety.

Conclusion

Thank you again for the opportunity to participate in today's discussion. And thank you for your leadership improving cybersecurity in the aviation sector. I look forward to working with you to strengthen the partnership between the public and private sectors and to share best practices to thwart future cyber attacks. I'm happy to answer any questions from the Committee.