Testimony of

Michael A. Stephens

General Counsel & Executive Vice President for Information Technology

Hillsborough County Aviation Authority

Tampa International Airport

Before the United States House of Representatives

Subcommittees on Cybersecurity and Infrastructure Protection

and

Transportation and Protective Security

"Understanding Cybersecurity Threats to America's Airlines"

September 6, 2018

Chairman Ratcliffe, Chairman Katko, Ranking Member Richmond, Ranking Member Coleman, and members of the Subcommittees, thank you for the opportunity to participate in this hearing on the critically important topic of understanding and mitigating cybersecurity threats to our nation's airlines, airports and national aviation system.

According to the Federal Aviation Administration (FAA), more than 2.5 million passengers fly in and out of America's airports each and every day. The most recent available statistics show US airports facilitated the shipment of more than 40 billion pounds of cargo. In total, our nation's airports along with our airline partners and all other aspects of the aviation industry contribute more than 5.1% to our national GDP. By any standard, airports, particularly our commercial airports are incredibly complex, connected critical infrastructure ecosystems that are essential not only to our nation's economic prosperity, but to our national security as well.

The size and scope of operations, as well as the passenger volume in our nation's airports is vast. The FAA classifies the nation's 30 largest airports by passenger volume, as large hub airports. Tampa International is in that category. Out of those 30 airports designated as large hubs, the top four or five have more passengers flowing through them on an annual basis than the entire population of the United States.

As with most industries, to meet the increasing demand and needs of international commerce and the traveling public, airports along with our airline partners, have increasingly relied on technology out of operational necessity and to enhance passenger safety, security and convenience. The ubiquitous use of technology has made airports, airlines and global aviation more efficient and has undergirded and facilitated the tremendous growth of global mobility, commerce and connectivity. However, as a result of our increasingly interconnected and technologically dependent world, airports and airlines, like other industries face significant challenges from a looming cyber threat environment.

In today's modern and technologically advanced airports, there are virtually no areas or functions that do not rely at some level on a digital network, data transfer, computer application or interface with the internet. Virtually all functions that are essential to airport operations, as well as aviation safety and security, such as access controls, navigation, airfield lighting, communications, industrial system controls, and emergency response systems rely heavily on a multitude of technology applications and platforms. Moreover, airport information systems contain or process tremendous amounts of sensitive data such as passenger manifests, security plans, and data containing financial and personally identifiable information (PII).

The operational importance of these systems coupled with the fact that they are often interconnected through networks and remote access points makes airports, immensely appealing

targets and potentially vulnerable to malicious cyber threats, such as criminal organizations and state sponsored actors.

Given the rapidly growing reliance on technology as well as the implementation of future technologies such as Next Generation Air Transportation System (NextGen) and remote air traffic control towers, it is my opinion that cybersecurity risks without question represent the preeminent and persistent threat to the continuous, safe, secure and efficient operations of US airports and the global aviation system.

One of the clearest examples of this threat to aviation safety and security was confirmed by the FBI and the Department of Homeland Security (DHS), Computer Emergency Readiness Team (CERT) earlier this year when they officially acknowledged that hackers attempted to penetrate the US civilian aviation, energy, and other critical infrastructure sector networks. CERT released a report on March 15 detailing what were believed to be state sponsored cyber efforts that targeted "US Government entities as well as organizations in the energy, nuclear, commercial facilities, water, aviation, and critical manufacturing sectors." The attempted attack was determined by intelligence assessments to be a sophisticated and coordinated assault that could have resulted, if successful, in significant potential disruptions to our critical infrastructure.

Imagine if you will, the potential dire consequences of a successful coordinated cyber-attack on any one or more of our large hub airports. The potential resulting disruption, chaos, and economic harm could be enormous. Consider the consequences of a single non cyber-related disruption that occurred at Atlanta International Airport in December 2017. In that instance, a power failure at Hartsfield-Jackson disrupted operations at the world's busiest airport, which resulted in the cancellation of more than 1,150 flights and stranded thousands of passengers in terminals and on planes for hours. The power failure at the airport, which moves more than 100 million passengers a year and serves as a major hub for domestic and international flights, led to additional disruptions across the country and affected flights in Chicago, Los Angeles and abroad.

The full economic impact resulting from this incident is still being fully assessed but conservatively the estimated losses in productivity as well as direct costs could be well in excess of $40 million. The power disruption in that instance was determined to have been caused by fire in a critical airport electrical node. However, had the incident been the result of a cyber-attack, the consequences of disruption, psychological impact and costs could have been far greater.

In short, computers, keyboards and kiosks have become the newest tools of criminals and the new weapons of war, and it is of paramount importance that we exercise increased urgency and vigilance to anticipate, identify and mitigate cyber threats to our nation's airlines, airports and aviation system critical infrastructure. Given the nature of these existing and growing threats, proactively implementing standards, protocols and counter measures to protect ourselves against potential catastrophic system disruption must be one of our highest priorities.

While there is no perfect defense against cybersecurity threats within the aviation industry or any industry for that matter, there are critical activities that we must undertake to mitigate as many risks as possible. For the purposes of this hearing, I have distilled my remarks down to three

critical areas that I believe present the best opportunity for airports along with our airline partners and aviation sector stakeholders to achieve greater preparedness, responsiveness and resilience.

Mandatory Minimum Standards

Under the Federal Information Security Management Act (FISMA), which defines a comprehensive framework to protect government information, operations and assets against natural or man-made threats, Federal agencies are required to adopt and implement a baseline national standard for cybersecurity preparedness. In 2013, President Obama issued Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity, which called for the development of a voluntary risk-based cybersecurity framework that is "prioritized, flexible, repeatable, performance-based, and cost-effective." Subsequent executive orders and Presidential Directives have also been issued to address and respond to the ever-changing cybersecurity threat landscape and strengthen the requirements by Federal agencies for ensuring and maintaining a baseline level of preparedness.

Although, airports, airlines and other aviation stakeholders have engaged in building and achieving various levels of cybersecurity capability, maturity and resilience, there are currently no significant requirements for adherence to minimum standards for preparedness. According to a survey of airports in the United States, by the Airport Cooperative Research Program (ACRP) as publish in 2015 in its Guidebook *on Best Practices for Airport Cybersecurity*, only nine out of twenty-four (34%) of airport respondents indicated that they had implemented a national cybersecurity standard or framework.

I believe that we are at a point in the growing threat environment where voluntary compliance is no longer adequate. I believe that strong consideration should be given by Congress and by regulatory agencies such as the FAA and Transportation Security Administration (TSA) which have primary responsibility for oversight and regulation of aviation operational safety and security respectively, to mandate the adoption and implementation of uniform minimum cyber security standards and frameworks. The National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure for Cybersecurity provides robust and comprehensive guidance for establishing minimum standards for the aviation sector.

Such a baseline cybersecurity framework would not replace an existing cybersecurity program that an organization already has in place. The framework would be used to augment, enhance and strengthen any existing program and align it with best practices for greater coordination and effectiveness throughout the aviation industry. For airports, airlines and key stakeholders that do not have a baseline cybersecurity program, such a requirement would ensure a minimum level of readiness and facilitate the development of greater preparedness and program maturity.

Cyber Security Information Sharing & Communication

While one of the stated objectives of EO 13636 focused on increasing information sharing between government and the private sector, it has not been as effective as it could be due to the voluntary nature of the program. The sharing of information and threat intelligence is a critical component to assessing airport and aviation sector vulnerabilities, enhancing our preparedness, as well as giving airports and our airline partners the ability to more effectively respond and recover in the event of a cybersecurity incident.

Often information sharing practices within the aviation sector have been reactive versus proactive. A voluntary information sharing program may have arguable utility when reacting to and recovering from a cyber-incident, but often possesses minimized utility effectiveness in preventing an incident when not shared in a timely manner.

To strengthen information sharing, consideration should be given to requiring mandatory disclosure of cyber incidents that meet an agreed-upon threshold irrespective of whether or not the incident resulted in a data breach or system compromise. Information sharing standards should ideally address whom the information should be shared with and its confidentiality within the industry in line the protections currently afforded to airport System Security Information (SSI).

Recent laws such as the Cybersecurity Information Sharing Act (CISA) and the corresponding programs such as the DHS Cyber Information Sharing and Collaboration Program (CISCP), if coupled with the implementation of mandatory minimum standards within the aviation sector, may help to accelerate the progress of information sharing and collaboration. However, mandating a minimum common standard and enhancing opportunities to share critical cybersecurity threat intelligence in a timely manner, will ultimately result in greater industry wide capability to combat cyber security risks.

Information Security Awareness and Workforce Training

Notwithstanding the most effective program standards, technological cybersecurity defenses and threat intelligence information sharing efforts, the human factor remains the most highly exploited vector for penetrating cybersecurity defenses within the aviation sector.

Cybersecurity threat awareness and information security training programs for all airport, airlines and aviation industry employees is perhaps one of the most effective and cost-efficient ways of increasing airports and airlines cybersecurity readiness. The NIST “Framework for Improving Critical Infrastructure Cybersecurity” (NIST 2014) specifically indicates that cybersecurity awareness and training is a critical and indispensable component to an entity’s overall cybersecurity program.

Numerous resources are available for cybersecurity training at the federal, department, and state-level. According to the survey of airports in the United States, by the Airport Cooperative Research Program (ACRP) as published in 2015, 20 of 27 (74%) of the responding airports indicated that they engage in some form of employee information security awareness training. However, due to the multitude of differences within airport governance and organizational

structures, the scope, depth and quality of training may vary significantly from airport to airport. Numerous additional factors may also adversely impact the quality and scope of training such as availability of budgets, subject matter expertise and adequate buy-in from senior management. Adopting and requiring a uniform standard which establishes a minimum training requirement for airport, airlines and other aviation sector employees on a defined and reoccurring basis should be given strong consideration by Congress and appropriate aviation sector regulatory agencies such as the FAA and TSA.

Conclusion

Our nation's airports, airlines and other critical aviation infrastructure are heavily reliant on information technology and complex data networks to support the growing demands of our economic and strategic interests. As the adoption of current and future technologies increases to support the aviation sector both here and abroad, the threat of disruptive cyber-attacks on airports, airlines and critical aviation information systems and data will undoubtedly increase as well. Evolution towards a more effective, non-voluntary cyber risk mitigation strategy against this pernicious and imminent threat must be undertaken proactively and with a renewed sense of urgency. The need for increased assistance and improved regulatory oversight, as well as the urgent adoption and implementation of a baseline cybersecurity protection framework and standard for information sharing and workforce training, is absolutely essential to the nation's security and long-term economic prosperity.

Thank you again for the opportunity to testify before you today. I look forward to answering any questions you may have.