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

Committee on Transportation and Infrastructure

"The Evolving Cybersecurity Landscape:
Industry Perspectives on Securing the Nation's Infrastructure"

Thursday, November 4, 2021

Chairman DeFazio, Ranking Member Graves, and distinguished members of the Committee thank you for the opportunity to participate in today's hearing on the critically important topic of understanding and mitigating cybersecurity threats to our nation's critical infrastructure.

According to the Federal Aviation Administration (FAA), more than 2.9 million passengers travel through America's airports each and every day. Based on some of the most recent available data, US airports facilitated the shipment of more than 44 billion pounds of cargo. In total, our nation's airports, along with our airline partners and all other aspects of the US aviation industry, account for more than 5.2% of our national GDP, contribute $1.6 trillion in total economic activity and support nearly 11 million jobs. 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 activity in our nation's airports, are vast. The FAA classifies the nation's 30 largest airports by passenger volume as large hub airports, of which Tampa International is in that category. Out of those 30 airports designated as large hubs, the largest five have more passengers flowing through them on an annual basis than the entire population of the United States.

As with most industries in order to meet the increasing demand and needs of global commerce and the traveling public, airports, along with our airline partners, have increasingly relied on technology both out of operational necessity and to enhance passenger safety, security and convenience. The ubiquitous use of technology has made airports, airlines, and aviation more efficient and has undergirded and facilitated the tremendous growth of global mobility, commerce, and connectivity.

In today's modern and technologically advanced airports, there are virtually no areas or functions that do not interface with or rely on some level on a digital network, data transfer, computer application, or internet interface. Virtually all functions essential to airport operations and 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 increasingly supported and connected through networks that rely on global technology supply chains, makes airports immensely appealing targets and increasingly vulnerable to criminal organizations and state-sponsored bad actors.

Airports, airlines, and the aviation sector, like other industries, face significant challenges from a persistent and increasingly pernicious cyber threat environment. Imagine, if you will, the potentially dire consequences of a successfully coordinated major cyber-attack on any one or more of our large hub airports, airlines, or the Air Traffic Management System. The potential resulting national and international disruption, economic harm, erosion of safety, and degradation of vital aspects of our national defense capability would be enormous.

In short, computers, keyboards, and digital code have become the newest tools of criminals and some of the preferred weapons of war for nation-states and other US adversaries. That is why it is of paramount importance that we exercise increased urgency and vigilance to anticipate,

identify and mitigate cyber threats to our nation's airports, airlines, and other critical aviation infrastructure. Given the nature of these existing and growing threats, proactively implementing standards, protocols, and countermeasures to protect ourselves against potential catastrophic system disruption must become one of our highest priorities.

While there is no silver bullet or perfect defense against cybersecurity threats within the aviation industry or any industry for that matter, there are critical activities that we must undertake to increase our cyber resilience and mitigate as much risk as possible. For the purposes of this hearing, I have distilled my remarks down to a few 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 national baseline 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 recent 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 a minimum baseline set of standards for preparedness. According to a 2015 survey of airports in the United States by the Airport Cooperative Research Program (ACRP) in its Guidebook *on Best Practices for Airport Cybersecurity*, only nine out of twenty-four (34%) airport respondents indicated that they had implemented a cybersecurity standard or framework. Even assuming that the percentage has increased, given the voluntary nature of implementing a standard within the industry, there is no meaningful way to assess adoption, adequacy, or consistency.

Moreover, according to a 2018 SITA Air Transport Cybersecurity Insights report of aviation industry participants, only 41% of respondents identified cybersecurity as part of their top organizational risks. Only 42% of respondents planned to include cyber risk in their organizational critical risk assessments in 2021. Fewer than 35% of the responding organizations had a dedicated Chief Information Security Officer (CISO), which is essential to raising cybersecurity resilience as a priority to most executive and governance levels.

Given these numbers, I believe that the aviation sector is at an inflection point in the growing threat environment where voluntary compliance is no longer adequate. This position is clearly evidenced by the increasing sophistication and adverse impact on our economic and national security from attacks such as SolarWinds and Colonial Pipeline. It is my opinion that strong

consideration should be given by Congress and regulatory agencies such as the FAA and TSA to mandate the adoption and implementation of minimum baseline cyber security standards and frameworks throughout the aviation sector. The National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure for Cybersecurity, for example, provides substantial guidance for establishing a minimum cyber resilience framework for the aviation sector and other critical infrastructure sectors.

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 more effective sector cyber preparedness and maturity.

Cyber Security Information Sharing & Communication

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

Often information sharing practices within the aviation sector have been reactive versus proactive. Voluntary information-sharing programs have demonstrated utility when reacting to and recovering from a cyber-incident when shared in a timely manner. However, the exponentially growing threat landscape will require significantly more investment by the public and private sectors both nationally and internationally.

In order to strengthen information sharing, consideration should be given to requiring mandatory disclosure of cyber incidents that meet an agreed-upon threat threshold irrespective of whether or not the incident resulted in an actual data breach or system compromise. The information reporting and sharing requirement should focus on actionable threats and risks in order to minimize the data and information overload, or the creation of information "white noise".

Laws such as the Cybersecurity Information Sharing Act (CISA) and related 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 baseline common standard and enhancing opportunities to share critical cybersecurity threat intelligence in a timely manner within the aviation and across other critical infrastructure sectors will ultimately result in the greater national capability to combat cyber security risks.

Information Security Awareness Training and Workforce Development

Closing the human factors gap is a critical and integral part of a successful and effective cyber resilience strategy within all critical infrastructure sectors. 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. In a recent study by Airports Council International (ACI) of key aviation leaders and stakeholders, 87% of the respondents reported that social engineering attacks were the leading vector of cyberattacks.

Cybersecurity threat awareness and information security training programs for all airport, airlines, and aviation industry employees is perhaps one of the most efficient and cost-effective ways of increasing cybersecurity preparedness in the aviation sector. 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.

Airports, airlines, and the aviation sector take cybersecurity seriously and have implemented creative processes to educate staff and tenants to further enhance cyber awareness, hygiene and security. Numerous resources are increasingly being made 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), 20 of 27 (74%) of the responding airports indicated that they engage in some form of employee information security 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 breadth of training, such as availability of budgets particularly in a post COVID environment, lack of available subject matter expertise and adequate buy-in from senior management in prioritizing spending on resiliency efforts.

To combat the exponential growth of cyberattacks, we must make significant investments to develop cyber literacy and equip people with the necessary tools to detect and defend against bad actors. This will require efforts beyond typical awareness training and would ideally build on aviation's physical safety-and-security culture to develop a cybersecurity culture across all industry stakeholders.

Adopting and requiring a uniform standard which establishes a minimum baseline training requirement for airport, airlines and other aviation sector employees on a defined and reoccurring basis should be given significant consideration by the appropriate aviation sector regulatory agencies such as the FAA and TSA.

Workforce Development

We are losing the race for talent. Professionals, specifically within the aviation industry, with critical cybersecurity skills and competencies are in scarce supply. In the US, we have a critical shortage of cybersecurity talent such as software engineers, software developers and network

engineers. By some industry estimates, the US currently has a shortage of more than one million security experts, and that number is expected to grow significantly over the next decade. These essential skills are necessary to increase our cyber resilience and response capabilities and represent a significant risk to US national security and competitiveness.

We must invest in building future cyber capacity by identifying and recruiting highly sought-after talent and developing and retaining our current cyber workforce. In order to close the cybersecurity skills gap, substantial national public and private efforts should be undertaken to develop and expand the capabilities of current and future workforces. Particular focus should be placed on developing cyber competencies through high school and university education programs promoting science, technology, engineering, mathematics, and foreign language (STEM-L).

Conclusion

Our nation's airports, airlines, and other critical aviation infrastructure rely heavily on information technology and complex data networks to support the growing demands of our economic, strategic, and national security 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, improved regulatory oversight, and the urgent adoption and implementation of a baseline cybersecurity protection framework and standard for information sharing and workforce training are essential to the nation's security and long-term economic prosperity.