S. HRG. 118–737

AVIATION CYBERSECURITY THREATS

HEARING

BEFORE THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED EIGHTEENTH CONGRESS

SECOND SESSION

SEPTEMBER 18, 2024

Printed for the use of the Committee on Commerce, Science, and Transportation

Available online: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
61–950 PDF WASHINGTON : 2025

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED EIGHTEENTH CONGRESS

SECOND SESSION

MARIA CANTWELL, Washington, *Chair*

AMY KLOBUCHAR, Minnesota	TED CRUZ, Texas, *Ranking*
BRIAN SCHATZ, Hawaii	JOHN THUNE, South Dakota
EDWARD MARKEY, Massachusetts	ROGER WICKER, Mississippi
GARY PETERS, Michigan	DEB FISCHER, Nebraska
TAMMY BALDWIN, Wisconsin	JERRY MORAN, Kansas
TAMMY DUCKWORTH, Illinois	DAN SULLIVAN, Alaska
JON TESTER, Montana	MARSHA BLACKBURN, Tennessee
KYRSTEN SINEMA, Arizona	TODD YOUNG, Indiana
JACKY ROSEN, Nevada	TED BUDD, North Carolina
BEN RAY LUJÁN, New Mexico	ERIC SCHMITT, Missouri
JOHN HICKENLOOPER, Colorado	J. D. VANCE, Ohio
RAPHAEL WARNOCK, Georgia	SHELLEY MOORE CAPITO, West Virginia
PETER WELCH, Vermont	CYNTHIA LUMMIS, Wyoming

LILA HARPER HELMS, *Staff Director*
MELISSA PORTER, *Deputy Staff Director*
JONATHAN HALE, *General Counsel*
BRAD GRANTZ, *Republican Staff Director*
NICOLE CHRISTUS, *Republican Deputy Staff Director*
LIAM MCKENNA, *General Counsel*

CONTENTS

WITNESSES

APPENDIX

AVIATION CYBERSECURITY THREATS

WEDNESDAY, SEPTEMBER 18, 2024

U.S. SENATE,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC.

The Committee met, pursuant to notice, at 10:05 a.m., in room SR–253, Russell Senate Office Building, Hon. Maria Cantwell, Chair of the Committee, presiding.

Present: Senators Cantwell [presiding], Klobuchar, Markey, Peters, Duckworth, Tester, Rosen, Hickenlooper, Welch, Cruz, Thune, Fischer, Blackburn, Budd, Schmitt, and Capito.

OPENING STATEMENT OF HON. MARIA CANTWELL, U.S. SENATOR FROM WASHINGTON

The CHAIR. Good morning. The Senate Committee on Commerce, Science, and Transportation will come to order.

This morning we are having a hearing on aviation cybersecurity threats and I appreciate the witnesses being here today.

The reality is stark. Our aviation industry is under constant threat from cyber attacks—up 74 percent since 2020. With the aviation sector contributing more than 5 percent of our GDP—that is $1.9 trillion in total economic activity and supporting 11 million jobs—we have to wake up and take these aviation cybersecurity threats seriously.

As we saw in the 1990s when weakness in the power grid exposed the system to catastrophic failures, we had a similar situation as we are in today with aviation. Like with the utility industry the solution has to be a strong national standard for resiliency and organizations committed to the highest standard, whether that is voluntary as organizations or something stronger.

Because every time we witness these technology failures consumers are the ones who are left holding the bags. Let me share a recent example that hits very close to home.

Last month, SeaTac Airport—Seattle-Tacoma International Airport—was hit by a ransomware attack from Rhysida Group, forcing airport leaders to shut down various computer systems that run everything from ticketing to display boards to baggage claims, creating confusing environment for passenger and workers and, yes, delaying flights and some flight cancelations.

The display boards were down for a week. I personally ran through the airport trying to catch a flight, not sure if I was going to the right gate. I had something on my device but since all the boards were dark I had no idea whether I was really going to get

to my gate or if that would really be the gate. I am not sure we had—I thought we had a chart picture of that.

The displays were down for a week and employees had paper signs directing passengers on where to get to a gate. Check-in kiosks were down too, forcing passengers to wait in line for paper tickets.

Other passengers endured long waits at baggage claim. Airport staff manually sorted through the checked baggage in the terminal.

The airport's internal e-mail system and website went down and the attack group, which is believed to be a Russian organization, is now threatening to release personal data from airport employees unless the airport pays $6 million worth of bitcoin ransom.

While most systems are now back online 3 weeks later the airport's website and some internal human resource functions remain down today.

I appreciate everything Sea-Tac's Aviation Management Director Lance Lyttle, who is with us here today—I appreciate him being here to discuss the impacts of this event and lessons learned.

Sea-Tac's situation is not unique. Across the country we have seen troubling examples of cyber vulnerabilities in our aviation sector. In 2020 a hacker accessed international—internal systems at San Francisco International Airport.

2020, San Antonio airport had its website spoofed, and let us not forget the 2015 incident where hackers claimed he had accessed a United Airlines flight control system through the in-flight entertainment system.

That is why we are here today, to spotlight this issue and figure out what more needs to be done, and to let the traveling public know that Congress and the Federal Government are going to combat potential disruptions to their air travel and safety.

The FAA reauthorization bill, which was signed into law, included a subtitle strengthening cybersecurity including directing FAA to establish a process to track and evaluate aviation cyber threats, designating a cybersecurity lead at the agency, and just last year TSA and FAA both issued cybersecurity requirements for airports, airlines, and manufacturers.

I am grateful to have Marty Reynolds here today, a cybersecurity expert from American—Airlines for America, who is here to tell us about emerging threats to aviation cybersecurity and how the industry and government can respond, and cyber attacks and other recent technology outages in aviation like the NOTAM failure or Southwest mount down or the CrowdStrike outage have made it clear that brittle infrastructure will not cut it.

In the aftermath of the cyber attack at Sea-Tac, Port of Seattle Executive Director Steve Metruck said that business and government, "needs to invest in cybersecurity," and, "need to be prepared should a cybersecurity gain access to systems."

When airport and airline systems are compromised it also puts passengers' personal data at risk. For instance, in 2020 hackers stole the credit card information of over 2,000 passengers and cyber attacks on frequent flyer accounts are up 166 percent in just the past 3 months. The Sea-Tac incident created hardships for travelers like nonfunctioning flight status and, as I mentioned, delays in getting luggage, and it is easy to imagine a scenario where cyber

attacks coinciding with other events could cause more cancelations or delays.

Even in these difficult situations airlines must abide by their passenger commitments and requirements. Mr. Breyault is here from the National Consumer League to remind us of those resources passengers have when dealing with flight disruptions. This includes requirements for airlines to provide hassle-free refunds as mandated by the FAA reauthorization.

So thank you again to our panelists for being here. I look forward to your testimony and now I will turn to Ranking Member Cruz for his opening statement.

STATEMENT OF HON. TED CRUZ,
U.S. SENATOR FROM TEXAS

Senator CRUZ. Thank you, Madam Chair.

If cyber crime were measured as a nation it would be the third largest economy in the world, costing about $10 trillion every year, up from just $3 trillion 10 years ago.

It is a threat that the Federal Government must take seriously. The transportation sector is often targeted by cyber criminals. No mode of transportation is immune. A 2021 ransomware attack rendered inoperable the Colonial Pipeline, which carries about 45 percent of the East Coast's fuel.

Airlines, pilots' unions, and airports globally have also all been hacked. While the Port of Seattle recovers from the August attack, it appears travelers were largely spared from widespread disruptions.

I look forward to hearing from Sea-Tac Managing Director Lance Lyttle on how the airport responded and any lessons learned.

I will note that Mr. Lyttle spent 5 years working for the Houston airport system before going to Sea-Tac so I would like to extend a special welcome to him.

Airlines, airports, and avionics manufacturers invest heavily to fortify their technology systems and to protect data. Cyber defenses are expensive and ever evolving due to the nature of cyber threats. But we should be cautious about placing too much faith in more regulation and reporting requirements to protect us.

I am concerned about the dozens of potentially duplicative cybersecurity reporting requirements that regulated entities must already comply with. There may be a better or more effective way to keep critical infrastructure secure than more box checking compliance activities.

Skepticism about new compliance burdens is well founded. The Federal Government itself has a lousy track record of protecting data from cyber attacks.

Millions of Americans' data have been stolen in government hacks over the past 10 years and, yet, the law today gives the Federal Government more than double the amount of time a private entity has to report a cybersecurity incident.

In many cases Federal agencies have little understanding of how regulated industries work. For example, when the Transportation Security Administration first issued security directives on cybersecurity requirements for pipelines, many of the mandates were impractical and had been designed without any private sector input.

The TSA set unrealistic timelines for pipeline operators to effectively overhaul their cybersecurity practices, and applied cybersecurity requirements typically required for computers such as updating passwords to things like sensors that monitor pipeline processes.

TSA's security directives created so much confusion that the agency received an unprecedented number, more than 380, of alternate measure requests from operators. Had TSA used a regular rulemaking process with notice and comment rather than issuing directives to industry without input those mistakes might have been avoided.

On the subject of TSA, I am pleased the Committee is holding a hearing related to aviation security. But we should be looking more closely at TSA's operations as well. For example, more than a year ago I began an oversight investigation into why three mayors of left-wing sanctuary cities were using commercial airports to house thousands of illegal aliens.

Not surprisingly, the Biden-Harris administration continues their delay tactics and has yet to provide all of the information that I have requested.

The Department of Homeland Security, including TSA, has failed to produce documents and communications requested about the potential security threats illegal aliens pose to airports and airport facilities.

Additionally, the FAA has failed to provide requested communications between it and other Federal entities about the housing of illegal aliens at airports.

Separately, I worked with Senators Merkley and Kennedy on an amendment to the FAA reauthorization on TSA's use of facial recognition technologies at passenger checkpoints.

The TSA begged Members of Congress to allow for continued facial recognition with no guardrails.

Chair Cantwell, I know you offered to Senator Merkley to hold a hearing on this and other topics. I think that is a great idea.

The TSA and the DHS must be more collaborative in their work, especially their rulemaking. I look forward to hearing from today's witnesses on their experience working with the TSA on cyber issues and how we can do more to keep the aviation sector safe.

The CHAIR. Thank you, Senator Cruz.

Again, welcome to our witnesses today. We will start with you, Mr. Lyttle, and if you would please begin. Five minutes of comments.

STATEMENT OF LANCE LYTTLE, AVIATION MANAGING DIRECTOR, SEATTLE-TACOMA INTERNATIONAL AIRPORT

Mr. LYTTLE. Chair Cantwell, Ranking Member Cruz and members of the Committee, thank you for the opportunity to join you today.

My name is Lance Lyttle. I am the Aviation Managing Director for Seattle-Tacoma International Airport, which is owned and operated by the Port of Seattle.

As you know, the port recently experienced a cyber attack which we first identified on August 24. The attack and our responsive ac-

tions initially impaired some of our operations and inconvenienced passengers.

STA has one of the smallest footprints of any major airport in the Nation and was designed to serve approximately 30 million passengers, compared to the 52 million we will serve this year.

Additionally, we are undergoing a major renovation to better accommodate the traveling public. As a result, the impact to our passengers was magnified and we regret any inconvenience.

We have made significant progress in restoring services and systems. Importantly, at no point did this incident affect the ability to safely travel through our airport or the port's maritime facility.

We were able to remain operating by partnering with airlines, utilizing paper boarding passes for lower volume carriers on our common use systems, and coordinating with TSA and CBP.

In addition, port employees provided more than 4,000 hours to assist with operating and customer service. Our team was able to bring the majority of the impacted operational system back online within a week. Our internal investigation is ongoing, but we know we were victims of a ransomware attack by the criminal organization known as Rhysida.

As soon as we identified the unauthorized cyber activity we quickly isolated critical systems. While our efforts to stop the attack appear to have been successful, the threat actor was able to encrypt some of our computer systems and copy some data.

The matter is under criminal investigation by the FBI. Rhysida sought a of ransom payment but the port has decided not to pay.

On Monday they posted on their dark website a copy of eight files stolen from port systems and are seeking 100 bitcoins to buy the data.

We are currently reviewing the files published on the leaked site as well as others we believe were copied. We will notify any individual whose personal information has been compromised and provide appropriate support.

While we are still in the midst of our recovery efforts we have already identified a number of lessons learned.

First, even though we have robust cybersecurity systems in place, cyber criminals are always involved in their tactics and so we are continuing to work to further harden our cyber defenses, including strengthening our identity management and authentication protocols as well as enhancing our monitoring.

Second, I am incredibly proud of how our team sprung into action to keep our airport operating, especially over the busy Labor Day travel period.

We benefited greatly from partnership with airlines, Federal agencies, and our tenants. We also developed workarounds to keep people and bags moving. Many of those workarounds are quite effective and will go into our toolbox for future emergency responses.

Also, communication was key. We held daily conference calls, relied heavily on text messages, used temporary signage, and did a lot of in-person communications. None of this is revolutionary but it is important to have these options already planned for when technology becomes inaccessible.

Finally, I want to talk about our goal to be stronger after. We hope our internal investigation and third party after action report

will identify best practices to improve our resiliency, our emergency preparedness, and our incident response.

We will also share these learnings with peers throughout the aviation industry. Congress and Federal agencies can help our industry in the face of these ongoing threats.

Agencies should continue to prioritize the dissemination of timely, actionable cyber threat information and we welcome the engagement of congressional leaders to help improve information sharing of industrywide best practices.

Thank you again for your time, and I am happy to answer any questions.

[The prepared statement by Mr. Lyttle follows:]

PREPARED STATEMENT OF LANCE LYTTLE, AVIATION MANAGING DIRECTOR, SEATTLE-TACOMA INTERNATIONAL AIRPORT

Chair Cantwell, Ranking Member Cruz, and members of the Committee, thank you for the opportunity to join you today. My name is Lance Lyttle, and I serve as the Aviation Managing Director for Seattle-Tacoma International Airport (SEA), which is owned and operated by the Port of Seattle.

The Port of Seattle is a special-purpose local government representing the residents of King County, Washington. In addition to SEA, the Port owns a major maritime gateway that includes international and domestic cargo operations, the largest cruise business on the West Coast, the homeporting of the North Pacific Fishing Fleet, and a variety of commercial and recreational boating marinas. SEA is the 11th busiest airport in the country by passenger volume, and the top ranked airport in the country three years in a row according to Skytrax.

We are here today because the Port recently experienced a cyberattack. While the incident has impacted our operations, we have made significant progress restoring services and systems. Importantly, at no point did this incident affect the ability to safely travel to or from Seattle-Tacoma International Airport or safely use the Port of Seattle's maritime facilities. Safety and security are our number one priority in response to this incident.

Alongside these restoration efforts, our own internal investigation is still ongoing. Our goal is to be transparent about this incident, but timing is critical. We are still investigating what data the threat actor obtained from our systems, and we are actively supporting the Federal Bureau of Investigation's (FBI) investigation of the incident. For these reasons, there is limited technical detail I can share at this time. We fully understand the importance of this information, and we are invested heavily in both understanding more about what happened and what lessons there are. To that end, we have engaged cybersecurity experts to conduct a forensic investigation, and we will be conducting an after-action review of this incident that will result in new information and insights.

In the interim, there are a number of lessons learned that we have already identified, which I am pleased to be able to share with you today. In particular, we are very proud of how Port employees and our partners came together to maintain continuity-of-operations throughout this incident, meaning that many of our passengers have had a relatively normal experience through the airport and our cruise terminals. I hope that my testimony today will help reassure air travelers of the safety, security, and resiliency of the aviation system.

Before I share some of those insights, I want to provide you with additional details about the incident. This incident was discovered when the Port of Seattle noticed unauthorized activity in our systems on August 24. It was a fast-moving situation, and Port staff worked to quickly isolate critical systems. However, both the attack itself and our responsive actions hindered some Port services, particularly at the airport—including access for some airlines to the baggage source messaging system, the check-in kiosks, common use ticketing, public Wi-Fi, airport display boards, the Port of Seattle website, the flySEA app, and reserved parking. Similarly, some of the systems on our cruise and marina side were impacted as well. Of note, the proprietary systems of our major airline and cruise partners were not affected, nor were the systems of our Federal partners like the Federal Aviation Administration (FAA), Transportation Security Administration (TSA), and U.S. Customs and Border Protection (CBP).

Thankfully, we were able to keep most airport passengers on track by working with their airlines; by utilizing paper boarding passes and baggage tickets for the

international carriers and lower volume carriers who rely on our common use system; and thanks to close coordination with TSA and CBP. I am very proud of the dedication, expertise, and resiliency of our employees, who demonstrated incredible knowledge of primary systems, backup systems, and manual systems. In addition, we are grateful to the Port employees from throughout our aviation and maritime divisions who contributed more than 4,000 hours over a ten-day period to help with operations, customer service, and wayfinding. For example, during the first days of the event, over 7,000 pieces of luggage were moved manually until some airlines regained the ability to access the baggage source messaging system.

Although there were some delays—particularly when a part of the baggage system was down—the airport has been able to successfully maintain regular operations. In addition, our team was able to bring the majority of the airport's operational systems back online within a week. Similarly, every cruise vessel left on time, and no travelers missed their sailings because of this incident.

Since August 24, Port staff have also been working with our technology partners and our forensics specialists to understand what happened, and we have been actively supporting law enforcement's investigation of the attack. As we shared publicly last week, we know that we were victims of a ransomware attack by the criminal organization known as Rhysida. While the efforts our team took to stop the attack appear to have been successful and there has been no new unauthorized activity since that day, our investigation has determined that the unauthorized threat actor was able to encrypt some of our computer systems and to copy some data from the environment.

As is typical in a ransomware attack, the threat actor sought to extort a ransom payment from the Port in exchange for providing a decryption key and deleting data they copied. On Monday, the threat actor posted the Port of Seattle's name on their leak site where they identify victims, as well as a copy of eight files stolen from Port systems. They plan to publish others in seven days unless we pay 100 bitcoin.

We are currently working to review the files published on the leak site as well as others we believe the actor copied. We will notify any individual whose personal information has been compromised, and will provide appropriate support. Fortunately, the Port has been able to validate that its backups were largely intact, and that no decryption key is necessary to restore our full operations.

The Port of Seattle has made the decision not to pay the perpetrators behind the cyberattack on our network. Paying ransomware to a criminal organization does not reflect Port values nor our commitment to be a good steward of public dollars. While we believe strongly this is the right approach, I can assure you that we take our employees' privacy very seriously, and this is not a decision that we take lightly. If we find that any employee's or individual's personal information has been compromised, we will notify them and provide appropriate support.

As I mentioned earlier, we are commissioning an independent after-action review and are continuing our own internal investigation. I look forward to being able to share additional details that we learn from our ongoing efforts. We also plan to share lessons learned with our peers throughout the aviation industry and others who operate critical infrastructure. And so, the insights that I am about to share are only preliminary.

In particular, I want to hit on three topics: 1) the effectiveness of cybersecurity systems, 2) the processes and practices that can ensure resiliency when faced with these issues, and 3) the Port's goal to be "stronger after" by incorporating these best practices into our future systems and plans.

We designed a robust IT and cybersecurity infrastructure to protect our systems from attack, and have received good feedback on both internal and external audits. Our staff is well-certified, experienced, and trained, and we have successfully detected attempts from some of the most advanced cyber attacks because of the strong program we had in place.

But there is no impenetrable cyberdefense, not only because cybercriminals are always evolving their tactics but also because an organization's protections are only as strong as the individuals who work within the system. Anyone who clicks on the wrong link, opens the wrong e-mail, or connects to the wrong Wi-Fi is a risk—no matter how many annual trainings they are required to attend or multi-factor authentications (MFA) they are required to enter. We think that critical infrastructure and other organizations will face increasingly sophisticated cyber attacks. In our region alone, just in the last few months the Seattle Public Library and the Highline Public Schools were shut down because of cyberattacks.

Overall, airports take cybersecurity seriously, and have allocated significant resources to these efforts; major airport cybersecurity programs include a variety of policies, procedures and controls designed to identify and protect key assets, as well as respond to potential incidents. Examples include targeted messaging and training

to raise cyber awareness throughout the airport; conducting penetration testing and vulnerability assessments; training and testing employees; and consulting with entities outside the aviation subsector to identify best practices and share lessons learned.

That said, there are definitely things we can do to further strengthen our security, and we regularly work to harden our cyber defenses. Our focus in the wake of this incident includes steps such as strengthening our identity management and authentication protocols, as well as enhancing our monitoring of our systems and network. For example, we have put greater protections around our active directory; made changes to keep our backup systems more secure and more quickly available; and added additional layers of restrictions so that major systems changes will have to go through additional layers of authorization.

Overall, we are learning the hard way about the pros and cons of separate systems versus vertical integration, the value and limitations of redundancies, and some of the technological workarounds that can quickly be put into place when main systems are offline. I want to thank our numerous external technology partners for their fantastic assistance during this incident—both to help us recover our systems and help us identify ways to build back better.

Second, in terms of resiliency, I am incredibly proud of our team for how they were able to spring into action and keep our airport operating, especially over the busy Labor Day travel period. The flights delays and cancellations in the initial few days of the incident were on par with a normal busy summer travel day. In fact, it is not an exaggeration to say that many travelers during this initial time period were unaware that we were having any problems at all, other than lack of access to public Wi-Fi and the fact that the Flight Information Display Systems (FIDS) and Baggage Information Display Systems (BIDS) were off.

Again, we benefitted greatly from incredible partnerships with airlines, Federal agencies, and our tenants. In addition, from manually moving baggage to writing boarding passes by hand, we found ways to ensure continuity-of-operations. Again, thank you to the Port employees who spent hours in the terminal answering questions from travelers and manually accomplishing tasks that are usually automated.

As I said, we have learned many lessons from going through this experience. For example, I mentioned earlier that we developed workarounds—both on the technology side and process-wise—to keep people and baggage moving; many of those workarounds are quite effective and will absolutely go into our toolbox for future emergency response best practices. In addition, one of the key takeaways for us is about the importance of communications with all of our airport stakeholders—especially when our employees are locked out of the systems that they normally use for communications, such as e-mail. There are tens of thousands of people who work at SEA on a daily basis—over and above the approximately 1,300 Port Aviation Division employees—and we need easily accessible ways to be able to update them regularly about what is working, what is still unavailable, and how to access information. During the first few weeks of this incident, we held daily teleconference calls, relied heavily on text message, used temporary signage, and did a lot of in-person communication. None of this is revolutionary, but when we have all become so reliant on technology it can be hard to readjust. For example, many airline ticketing agents and Transportation Security Officers had not seen or used a handwritten boarding pass, and so ensuring that this approach worked was a conversation with many parties.

On a related note, we have also established and strengthened a number of cybersecurity relationships that will be incredibly beneficial in the future. For example, some of our systems like the FIDS rely on airline data, and our airline partners wanted to be sure that our systems were truly secured before they re-connected; this discussion involved strengthening our high-level conversations with the cybersecurity leadership of their organizations. Similarly, we have received fantastic outreach from key Federal agencies like the Cybersecurity and Infrastructure Security Agency (CISA); they have always been a great partner, but this incident has brought us closer together and opens the door to long-term collaboration opportunities such as better sharing of best practices and improving workforce development.

Finally, I want to talk about our goal to be "stronger after." Recovering from this incident has involved rebuilding some major Port systems from scratch, and it is not lost on me that we are doing work to restore and build systems that would normally take years to do, yet we are accomplishing things in a matter of weeks. Our technology partners have been fantastic at helping us build in better cybersecurity protections from the ground up as we do so.

It is essential that we learn as many lessons as possible from this challenging experience, and we are very hopeful that our continuing internal investigation and our

third-party after-action review will help us identify additional best practices to improve our resiliency, our emergency preparedness, and our incident response.

Importantly, we do not want any other airport to have to go through what we are dealing with, and so we are dedicated to sharing best practices with peers throughout the aviation industry. We look forward to working with the Airports Council International, the American Association of Airport Executives, Airlines For America, CISA, the U.S. Department of Homeland Security, and many others to enhance the security of our collective operations. We have already begun conversations with TSA's Aviation Security Advisory Committee about how to utilize their forum, especially because TSA is the main regulator of airport cybersecurity. I want to be sure to call TSA out for being fantastic partners during this incident—both on the operational and the regulatory side.

I want to conclude by speaking briefly about ways that Congress and Federal agencies can help the aviation industry be even more resilient in the face of these ongoing threats and challenges. In particular, government agencies should continue to proactively prioritize the dissemination of timely and actionable cyber threat information as soon as reasonably practicable; classified briefings should be provided at the earliest opportunity to highlight new and emerging threats.

In accordance with a TSA mandate, airports and airlines have been reporting cybersecurity incidents to CISA, and there are opportunities to improve the two-way sharing of information. The aviation industry benefits greatly from information about common cybersecurity incidents, and we need to make sure we are optimizing our security tools, talent, and properly resourcing our cyber ecosystems to focus mitigation efforts.

With that overview, I will end my remarks, and I welcome any questions you may have. Thank you again for your time, and for the invitation to be here today.

The CHAIR. Thank you.

Mr. Breyault, thank you and welcome.

STATEMENT OF JOHN BREYAULT, VICE PRESIDENT OF PUBLIC POLICY, TELECOMMUNICATIONS AND FRAUD NATIONAL CONSUMERS LEAGUE

Mr. BREYAULT. Good morning, Chair Cantwell, Ranking Member Cruz and distinguished members of the Committee. My name is John Breyault and I am the Vice President of Public Policy, Telecommunications, and Fraud at the National Consumers League.

Founded in 1899, NCL's nonprofit mission is to advocate on behalf of consumers and workers in the United States and abroad. Today I will address the serious impact cybersecurity incidents in the aviation industry have on passengers and urge the Committee to ensure that consumers are not left bearing the cost of these events.

When cybersecurity incidents occur in the airline industry passengers are often the ones who suffer the most. Flights are delayed or canceled, personal information is compromised, and families can find themselves stranded for days.

Recent incidents underscore how an error in one sector can create a cascading effect across the industry, harming millions of passengers.

Senator, as you mentioned, last month a cyber attack at Seattle-Tacoma International Airport resulted in significant disruptions, forcing staff to handwrite boarding passes and manually sort bags, creating delays in both departing flights and bags arriving at their destinations.

On July 18th a faulty update affecting CrowdStrike clients, including airlines, led to global system crashes, affecting an estimated 1.4 million passengers.

Nearly 5,200 flights were canceled on the first day alone. Families were left stranded with one family in Seattle reportedly losing

more than $7,500 while trying to rebook flights and cover lodging costs.

Government agencies are not immune to cyber incidents either. In early 2023 an FAA contractor's error resulted in a nationwide ground stop. More than 10,000 flights were delayed and over 1,300 were canceled, once again highlighting the fragility of airline infrastructure to human error and cyber vulnerabilities.

While cyber events that disrupt flights generate headlines, the vulnerability of airline rewards programs has the potential to affect even more consumers. The value of unused miles sitting in passengers' rewards accounts is staggering.

According to one estimate, the top five U.S. airline loyalty programs ended 2020 with a combined balance of $27.5 billion in unused loyalty program miles, up $2.9 billion from 2019.

Unsurprisingly, all of those unused miles are an attractive target for cyber thieves. Between the fourth quarter of 2023 and the first quarter of 2024, bot attacks on airline accounts increased 166 percent.

Stolen airline miles fuel a thriving market on the dark web where crooks redeem these stolen miles for gift cards or by purchasing airline tickets.

Despite this threat, U.S. airlines have been inconsistent in their efforts to secure mileage accounts. For example, basic account security tools like multi-factor authentication that are commonplace on other sensitive accounts like those for online banking are not available to all passengers.

To make matters worse, airline miles are not covered by any of the consumer protections that safeguard consumers' money in other contexts such as FDIC insurance or the Electronic Fund Transfer Act's anti-fraud protections.

Ransomware attacks are another vulnerability for the aviation sector. Boeing's chief security officer last year noted that ransomware attacks on the aviation supply chain jumped 600 percent in the past year.

TSA cited persistent cybersecurity threats against the aviation sector when it adopted emergency security amendments. In the face of these threats, there have been some limited efforts to promote additional investment in the aviation sector's cybersecurity resiliency but more remains to be done.

For example, TSA last year rolled out new rules that require airports and operators to develop cybersecurity plans, and industry bodies like IATA and A4A play a key role in developing cybersecurity standards for the industry.

While these efforts are laudable, no amount of investment will prevent all incidents and for this reason NCL urges DOT and Congress to take additional steps to protect passengers.

Specifically, Congress should pass comprehensive national data security standards legislation to create a baseline of protection for the data consumers share with the industry, including with airlines.

Second, the value of airline rewards should be protected from fraud. Just as consumers are not liable when bad actors run up credit and debit card charges so too should airlines be required to replace airline miles lost to cyber thieves.

Third, DOT should require airlines to clearly and promptly communicate to consumers what their rights are under Federal passenger protection laws in the event of cybersecurity-related delays and cancelations.

Finally, Congress should explicitly codify DOT's authority to promulgate delay compensation rules to ensure that consumers can obtain cash compensation if an airline cybersecurity incident results in a significant delay or cancelation.

Chair Cantwell, Ranking Member Cruz, members of the Committee, we are grateful for your continuing work to protect consumers and for holding this hearing.

On behalf of NCL, thank you for including the consumer's perspective as you consider these important issues. I look forward to answering your questions.

[The prepared statement of Mr. Breyault follows:]

PREPARED STATEMENT OF JOHN BREYAULT, VICE PRESIDENT OF PUBLIC POLICY, TELECOMMUNICATIONS, AND FRAUD, NATIONAL CONSUMERS LEAGUE

Introduction

Good morning Chair Cantwell, Ranking Member Cruz, and distinguished members of the Committee. My name is John Breyault and I am the Vice President of Public Policy, Telecommunications, and Fraud at the National Consumers League. Founded in 1899, the National Consumers League ("NCL") is the Nation's pioneering consumer and worker advocacy organization. Our non-profit mission is to advocate on behalf of consumers and workers in the United States and abroad.[1] On behalf of the NCL, I would like to extend our sincere appreciation to the Committee for giving me the opportunity testify. Today, I will address the serious impacts cybersecurity incidents in the aviation industry have on consumers and urge the Committee to ensure that consumers are not left bearing the costs of these events.

I. Recent Incidents Have Highlighted the Need for Action to Strengthen Cybersecurity Defenses and Reduce the Risk to Passengers

When cybersecurity incidents occur in the airline industry, consumers are often the ones who suffer the most. Flights are delayed or canceled, personal information is compromised, and families can find themselves stranded for days without recourse.

Recent incidents are emblematic of this impact, underscoring how interconnected airline systems are and how an error in one sector can create a cascading effect across the industry, harming millions of passengers.

Last month, a cyberattack on Seattle-Tacoma International Airport resulted in significant disruptions, affecting critical infrastructure including the baggage system, terminal screens, check-in kiosks, airport website, and even communication systems such as phone and e-mail.[2] While larger airlines operating at Sea-Tac, such as Delta and Alaska Airlines, suffered fewer consequences, smaller carriers like Frontier, Spirit, Sun Country and all international airlines were among those especially affected because they do not have their own dedicated systems within the airport. Staff at affected airlines were forced to handwrite boarding passes and luggage tags for passengers and manually sort bags to their proper gates and baggage claims. This led to delays in both departing flights and bags arriving at their destinations.[3]

On July 18, a faulty update affecting CrowdStrike clients, including airlines, led to global system crashes, affecting an estimated 1.4 million passengers,[4] nearly

[1] For more information, visit *www.nclnet.org.*

[2] Kapko, Matt. "Seattle Airport Targeted in Cyberattack over Labor Day Weekend." *Cybersecurity Dive,* 5 Sept. 2024, *www.cybersecuritydive.com/news/seattle-airport-cyberattack-labor-day/725772/.*

[3] Brenda, David. "SeaTac Airport Outage Is Ongoing: Here's What Travelers Should Know." *Washington State Standard,* 27 Aug. 2024, *https://washingtonstatestandard.com/2024/08/27/seatac-airport-outage-is-ongoing-heres-what-travelers-should-know/.*

[4] Weston, David. "Helping Our Customers Through the CrowdStrike Outage." *Microsoft Blog,* 20 July 2024, *https://blogs.microsoft.com/blog/2024/07/20/helping-our-customers-through-the-crowdstrike-outage/;* Oxford Economics. "CrowdStrike Update Grounds Thousands of Flights."

Continued

5,200 were canceled on the first day alone.[5] Delta Air Lines canceled 7,000 flights over a five-day span.[6] Families were left stranded, with one family in Seattle reportedly losing more than $7,500 while trying to rebook flights and cover lodging costs.[7]

While the CrowdStrike outage was not caused by malicious actors, hackers did reportedly take advantage of the chaos caused by the incident. They launched phishing attacks trying to trick people into downloading malware, divulging security credentials, or making financial payments. Fake websites arose fraudulently impersonating CrowdStrike. CrowdStrike also disclosed that hackers were circulating a malicious ZIP file largely targeting Latin American customers.[8]

Cyber threats are not confined to American air carriers. A 2021 data leak at Air India allowed cyber attackers to access systems for more than three weeks at the carrier's Atlanta data center, affecting approximately 4.5 million customers.[9] A May 2020 hack of British carrier EasyJet compromised the e-mail and travel details of around 9 million customers, and the credit card details of more than 2,000 of them.[10] And a 2018 breach at British Airways stemming from a third-party cargo handler affected nearly a half million customers, with almost 250,000 individuals having their names, addresses, payment card numbers, and CVV numbers taken.[11]

Government aviation safety agencies are not immune to cyber incidents either. In early 2023, a contractor inadvertently deleted critical files while updating a database for the Federal Aviation Administration ("FAA"), causing a nationwide ground stop. More than 10,000 flights were delayed and over 1,300 were canceled, once again highlighting the fragility of airline infrastructure to human error and cyber vulnerabilities.[12] Although the FAA has since implemented backup systems to reduce the risk of such failures, the incident illustrates how vital resilient systems are for maintaining public trust and ensuring consumer protection.[13]

II. Cyber Vulnerability of Airline Rewards Programs Is of Particular Concern to Consumers

While cyber events that disrupt flights generate headlines, the vulnerability of airline rewards programs has the potential to affect even more consumers.

As billions of dollars worth of points flow in and out of mileage programs annually, rewards programs are increasingly seen as easy pickings by hackers. The value of unused miles sitting in passengers' rewards accounts is staggering. According to a 2018 McKinsey report, more than 30 trillion frequent-flier miles were sitting unspent in accounts. That was enough to let almost every airline passenger in the world redeem miles for a free one-way flight.[14] Other estimates put the value of unredeemed miles for U.S. airlines at a lower, but still significant valuation. Accord-

---

Oxford Economics, July 23, 2024, *https://www.oxfordeconomics.com/resource/crowdstrike-update-grounds-thousands-of-flights/*.

[5] Whitmore, Geoff. "The CrowdStrike Outage Is Still Impacting Airlines." *Forbes,* 22 July 2024, *www.forbes.com/sites/geoffwhitmore/2024/07/22/the-crowdstrike-outage-is-still-impacting-airlines/*.

[6] Draper, Kevin. "Delta Airlines Still Recovering from CrowdStrike Outage." *The New York Times,* 13 Sept. 2024, *www.nytimes.com/2024/09/13/travel/crowdstrike-outage-delta-airlines.html.*

[7] Tran, Louie. "Seattle Family Stranded Multiple Days after Delta Cancels Flights amid CrowdStrike Outage." *KIRO 7 News,* 14 Sept. 2024, *www.kiro7.com/news/local/seattle-family-stranded-multiple-days-after-delta-cancels-flights-amid-crowdstrike-outage/CFNOKCMRGRB5FNL2ZIUVW5ZW5A/*.

[8] DeNardis, Laura. "Is Global Tech Infrastructure Too Vulnerable? Professor Responds to CrowdStrike. Microsoft Outage," Georgetown University, 25 July, 2024, *https://www.georgetown.edu/news/ask-a-professor-crowdstrike-outage/*

[9] "India's Massive Cyberattack Hits Airline Operations." *BBC News,* 22 May, 2021, *https://www.bbc.com/news/world-asia-india-57210118;* Sinha, Saurabh. "Air India Data Breach: SITA Says Cyber Attackers Accessed Some Systems for 22 Days at Atlanta Centre." *The Times of India,* 22 May, 2021, *https://timesofindia.indiatimes.com/india/air-india-data-breach-sita-says-cyber-attackers-accessed-some-systems-for-22-days-at-atlanta-centre/articleshow/82864982.cms.*

[10] Holton, Kate. "EasyJet Cyberattack Hits Operations." *Reuters,* 21 July 2024, *www.reuters.com/article/easyjet-cyber-idUSFWN2D10F5/*.

[11] Information Commissioner's Office. *British Airways Penalty Notice.* 16 Oct. 2020, *www.ico.org.uk/media/action-weve-taken/mpns/2618421/ba-penalty-20201016.pdf.*

[12] Shepardson, David *et al.* "U.S. FAA Says Flight Personnel Alert System Not Processing Updates after Outage." *Reuters,* 11 Jan. 2023, *www.reuters.com/business/aerospace-defense/us-faa-says-flight-personnel-alert-system-not-processing-updates-after-outage-2023-01-11/*.

[13] Heilweil, Rebecca. "After 2023 Outage That Paused Flights Nationwide, FAA Now Has Backup System." *FedScoop,* 21 Sept. 2024, *https://fedscoop.com/after-2023-outage-that-paused-flights-nationwide-faa-now-has-backup-system/*.

[14] Saxon, Steve and Spickenreuther, Thorsten. "Miles Ahead: How to Improve Airline Customer Loyalty Programs." *McKinsey & Company,* 10 Oct. 2018, *www.mckinsey.com/industries/travel-logistics-and-infrastructure/our-insights/miles-ahead-how-to-improve-airline-customer-loyalty-programs.*

ing to ValuePenguin, a consumer research website, the top five U.S. airline loyalty programs ended 2020 with a combined balance of $27.5 billion in unused loyalty program miles, up $2.9 billion from 2019.[15]

Unsurprisingly, all of those unused miles are an attractive target for bad actors. Between the fourth quarter of 2023 and the first quarter of 2024, bot attacks on airline accounts increased 166 percent, according to cybersecurity firm Arkose Labs.[16] The Loyalty Security Alliance, a travel industry group, estimates that successful hacks of rewards accounts have increased by 30–40 percent.[17] Experts state that roughly 1 percent of airline point redemptions are fraudulent, with total losses amounting to about 3 percent when associated costs, such as staff time and the refunding of points to some customers are included.[18]

Stolen airline miles fuel a thriving market on the dark web and other black markets where buyers redeem stolen points for gift cards or by purchasing airline tickets. Some of the hacked accounts are used to sell discounted airline tickets to the public on websites that are made to resemble legitimate travel agencies.[19]

The airlines need to do a better job of securing consumers' valuable miles accounts. Despite the well-known attractiveness of airline rewards to hackers, U.S. airlines have been inconsistent in their efforts to secure these accounts. Basic account security tools, like multi-factor authentication ("MFA"), that are commonplace on other sensitive accounts, like those for online banking, are not available to all passengers. While American Airlines began phasing in MFA in 2023,[20] it appears that United and JetBlue only began implementing MFA in recent months.[21] Neither Southwest nor Delta appear to offer MFA for their customers' rewards accounts.

To make matters worse, airline miles accounts are not covered by any of the consumer protections that safeguard consumers' money in other contexts, such as FDIC insurance or the Electronic Fund Transfer Act's anti-fraud protections. The Internet is littered with stories of consumers whose rewards accounts have been hacked and who then must spend hours on the phone with airlines and other rewards providers to try and get their miles back.[22]

III. Recent Incidents Are Part of a Troubling, Industrywide Trend

The cyber incidents mentioned above may have been isolated, but taken together, they are part of a larger, growing trend. Ransomware attacks, in particular, are a widespread and increasing concerns for stakeholders in the aviation sector.

A recent report from cybersecurity consulting firm Bridewell found that 55 percent of civil aviation organizations were targeted by ransomware in the past 12 months. Of these, more than four-in-ten (41 percent) said that loss of data was one of the primary consequences and 38 percent pointed to operational disruption. More

---

[15] Greenberg, Peter. "Airline Loyalty Programs Getting Harder to Redeem Frequent Flyer Miles." *CBS News,* 20 June, 2022, *www.cbsnews.com/news/airline-loyalty-programs-getting-harder-to-redeem-frequent-flyer-miles/*.

[16] Arkose Labs. "The Wiretap: Hackers Want Your Airline Miles." *Arkose Labs,* 2 July 2024, *www.arkoselabs.com/latest-news/the-wiretap-hackers-want-your-airline-miles/*.

[17] "Hackers Are Now Coming For Your Airline Miles And Hotel Points," *Forbes,* June 28, 2024, *https://www.forbes.com/sites/jeremybogaisky/2024/06/28/airline-miles-hotel-points-hacking/*.

[18] Bogaisky, Jeremy. "Hackers Are Stealing Airline Miles and Hotel Points, and Banks Aren't Coming to Your Rescue." *Forbes,* 28 June 2024, *www.forbes.com/sites/jeremybogaisky/2024/06/28/airline-miles-hotel-points-hacking/*.

[19] Bogaisky, Jeremy. "Airline Miles, Hotel Points Hacking: What Travelers Need to Know." *Forbes,* 28 June 2024, *www.forbes.com/sites/jeremybogaisky/2024/06/28/airline-miles-hotel-points-hacking/;* Bischoff, Paul. "How Much Are Stolen Frequent Flyer Miles Worth on the Dark Web?" *Comparitech,* 15 Nov. 2018, *www.comparitech.com/blog/information-security/how-much-are-stolen-frequent-flyer-miles-worth-on-the-dark-web/*.

[20] Leff, Gary. "American Airlines Rolling Out Required Multifactor Authentication to Access AAdvantage Accounts." *View from the Wing,* 20 June 2023, *https://viewfromthewing.com/american-airlines-rolling-out-required-multifactor-authentication-to-access-aadvantage-accounts/*.

[21] "2FA Finally Available." *Reddit,* April 2024, *www.reddit.com/r/unitedairlines/comments/1c6jbko/2fa_finally_available/;* WandrMe. "Status Update." *X* (formerly Twitter), 15 Sept. 2024, *https://x.com/WandrMe/status/1803891483441008787*

[22] Henderson, Clint. "My AAdvantage Account Was Hacked—Here's What I Did Next." *The Points Guy,* 19 Apr. 2024, *www.thepointsguy.com/news/hacked-aadvantage-account/;* Adams, Kurt. "What to Do If Your Points or Miles Are Stolen." *Going,* 5 Apr. 2024, *www.going.com/guides/points-miles-stolen;* Sweet, Joni. "Hackers Can Steal Your Frequent Flier Miles—How to Protect Your Travel Loyalty Accounts." *Frommer's,* 12 May, 2023, *www.frommers.com/tips/airfare/hackers-can-steal-your-frequent-flier-mileshow-to-protect-your-travel-loyalty-accounts;* "Hackers Stealing Hard-Earned Travel Loyalty Points." *Central Oregon Daily News,* 31 July, 2024, *www.centraloregondaily.com/news/consumer/hackers-stealing-hard-earned-travel-loyalty-points/article_d6a77a14-4f67-11ef-9e51-933d75667c96.html.*

than a quarter (28 percent) said the financial losses from paying a ransom were a consequence of the attacks.[23]

Boeing's Chief Security Officer Richard Puckett last year noted that ransomware attacks on the aviation supply chain jumped 600 percent in the past year.[24] One notable attack in 2023 targeted Boeing with a $200 million ransom demand.[25] The Transportation Security Administration ("TSA") cited "persistent cybersecurity threats against . . . the aviation sector" when adopting emergency amendments to certain security programs last year.[26]

The threats described above are not unique to the airline sector. While ransomware attacks targeted 55 percent of civil aviation organizations in the last 12 months, this compares favorably with other critical infrastructure sectors. For example, another survey by Bridewell found that over the same time period, 78 percent of financial services firms, 76 percent of firms in the rail sector, 71 percent of Federal government organizations, and 60 percent of firms in the energy sector had experienced ransomware attacks.[27]

This finding is supported by similar data from the World Economic Forum, finding that among critical infrastructure sectors targeted by cybercrime activity, healthcare is most affected, followed by financial infrastructure, telecommunications, and then transportation.[28]

IV. Action to Spur Cybersecurity Investment Would Benefit Passengers

There have been some limited efforts to prompt additional investment in the aviation sector's cybersecurity resiliency, but more remains to be done.

For example, Section 395 of the Federal Aviation Administration Reauthorization Act of 2024 directed the FAA Administrator to convene a Civil Aviation Cybersecurity Rulemaking Committee within one year of enactment. The committee will be tasked with making findings and recommendations on cybersecurity standards for civil aircraft, aircraft ground support information systems, airports, ATC mission systems, and aeronautical products and articles.[29] Last year, the Transportation Security Administration rolled out new rules that require airports and operators to develop cybersecurity plans and obtain TSA approval of the plans. This follows on the heels of TSA rules directing airports and airlines to designate a cybersecurity coordinator, report cybersecurity incidents to the Federal government within 24 hours, develop cyber incident response, and conduct vulnerability assessments.[30]

Industry bodies, such as the International Air Transport Association, also play a key role in developing cybersecurity standards for the aviation industry.[31] In the U.S., industry groups, led by Airlines for America, have been at the forefront in advocating for greater harmonization of cybersecurity regulations.[32]

---

[23] Bridewell Consulting. *US CNI Research Report 2024: Cyber Security in Aviation.* 12 Aug. 2024, *https://insights.bridewell.com/l/838563/2024-08-12/bq8xv/838563/17234559391WNSYJDg/US_CNI_Research_Report_2024_Cyber_Security_in_Aviation.pdf.*

[24] Boynton, Christine. "Cybersecurity Threats in Aviation: Bolstered Efficiency and Geopolitics." *Aviation Week,* 20 April, 2023, *www.aviationweek.com/air-transport/airlines-lessors/cybersecurity-threats-aviation-bolstered-efficiency-geopolitics.*

[25] Vicens, AJ. "Boeing Confirms Attempted $200 Million Ransomware Extortion Attempt." *CyberScoop,* 8 May 2024, *www.cyberscoop.com/boeing-confirms-attempted-200-million-ransomware-extortion-attempt/.*

[26] Transportation Security Agency. "TSA Issues New Cybersecurity Requirements for Airports and Aircraft." 7 Mar. 2023, *www.tsa.gov/news/press/releases/2023/03/07/tsa-issues-new-cybersecurity-requirements-airport-and-aircraft.*

[27] Bridewell Consulting. *US CNI Research Report 2024: Cyber Security in Aviation.* 12 Aug. 2024, *https://insights.bridewell.com/l/838563/2024-08-12/bq8xv/838563/17234559391WNSYJDg/US_CNI_Research_Report_2024_Cyber_Security_in_Aviation.pdf.*

[28] Joshi, Akshay. "Cybercrime Target Sectors: Latest Cybersecurity News." *World Economic Forum,* 24 Apr. 2024, *www.weforum.org/agenda/2024/04/cybercrime-target-sectors-cybersecurity-news/.*

[29] FAA Reauthorization Act of 2024. Sec. 395. *https://www.congress.gov/bill/118th-congress/house-bill/3935/text*

[30] Starks, Tim. "U.S. Government Debuts New Cyber Rules for Aviation Sector." *The Washington Post,* 8 Mar. 2023, *www.washingtonpost.com/politics/2023/03/08/us-government-debuts-new-cyber-rules-aviation-sector/.*

[31] International Air Transport Association. *Cyber Security in Aviation: Industry Position 2023.* IATA, 2023, *www.iata.org/contentassets/f23f6fa53f6b4dff8178bf88102c9f09/acysec-industrypositon-2023.pdf.*

[32] The White House. *Cybersecurity Regulatory Harmonization RFI Summary.* June 2024, ("In their responses, Airlines for America (A4A) and the Association of American Railroads (AAR) advocated for adopting standardized cybersecurity frameworks to ensure that regulation improves cybersecurity outcomes, not merely increases compliance costs.") *www.whitehouse.gov/wp-content/uploads/2024/06/Cybersecurity-Regulatory-Harmonization-RFI-Summary-ONCD.pdf.*

While these efforts are laudable, no amount of cybersecurity investment can prevent all incidents that impact passengers. It is for these reasons that NCL urges the U.S. Department of Transportation ("DOT") and Congress to take additional steps to reduce the harm that cybersecurity incidents cause to consumers. Specifically:

- Congress should pass comprehensive national data security standards legislation. NCL has long supported such legislation to give consumers a baseline of protection for the data that they share with industry, including with airlines;
- The value of airline rewards should be protected from fraud. Just as consumers are not liable when bad actors compromise their credit and debit card accounts and run up charges, so too should airlines be required to replace airline miles lost to cyberthieves; and
- Congress should explicitly codify DOT's authority to promulgate delay compensation rules and ensure that the forthcoming rules allow consumers to obtain cash compensation if an airline cybersecurity incident results in a significant delay or cancellation.

Conclusion

Chair Cantwell, Ranking Member Cruz, and members of the committee, we are grateful for your continuing work to protect consumers and for holding this hearing. On behalf of the National Consumers League, thank you for including the consumer perspective as you consider these important issues.

The CHAIR. Thank you so much, and we will look forward to digging in on a myriad of those issues you brought up.

Brigadier General Reynolds, thank you so much. I think you probably had plans to be at a different conference today but thank you for being here.

STATEMENT OF MARTY REYNOLDS, BRIGADIER GENERAL, USAF (RETIRED), MANAGING DIRECTOR FOR CYBERSECURITY, AIRLINES FOR AMERICA

General REYNOLDS. Thank you, and this is important so I am glad to be here.

Chair Cantwell, Ranking Member Cruz, members of the Committee, thank you for the opportunity to testify on the critical issue of aviation cybersecurity.

I would also like to thank my fellow panel members, Mr. John Breyault and Mr. Lance Lyttle, for their participation as well.

I am Marty Reynolds, the managing director for cybersecurity at Airlines for America. I have been with Airlines for America for three years and spent nearly three decades in the military, including time developing cyber policies and leading cyber professionals executing global operations.

I can tell you firsthand that our air carriers fully recognize that cybersecurity is one of the greatest challenges facing all critical infrastructure sectors.

The capability and capacity of threat actors operating in cybersecurity is growing at an alarming rate and there are no silver bullets in cybersecurity. To counter these many threats our carriers have developed mature cybersecurity programs that are risk-based, threat informed, and constantly evolving to stay ahead of a dynamic threat landscape.

Our members' cybersecurity programs and investments are based on these foundational principles. Our North Star will always be the safety, security, and privacy of passengers and crew. They are our industry's highest priorities.

This is why our industry continues to make significant investments in information technology infrastructure and cybersecurity. As an example, from 2018 to 2023 U.S. passenger airlines spent approximately $36.5 billion on information technology and cybersecurity, including $7.4 billion in 2023 alone.

Our members participate in and lead the development and updating of critical information technology and aviation cybersecurity standards. At A4A we created a cybersecurity council consisting of the cyber or the chief information security officers or vice presidents of Aviation Information Technology where we create industry best practices and lessons learned.

And, last, we consistently engage and collaborate with Federal departments and agencies to ensure we understand their policies and regulatory objectives so we can ensure we are compliant with the requirements.

While a good foundation exists, there is always room for improvement. Specifically, in addition to the increasing change in the threat landscape we have also seen a significant increase in regulatory requirements over the past three years.

This has created a complex compliance framework for airline operators and can divert critical resources away from cybersecurity teams.

However, we believe that there are opportunities to address these complexities through a couple of recommendations.

First, the Federal Government should continue to find ways to harmonize its cybersecurity requirements. As an example, airline operators are responsible to 10 different Federal agencies and departments with existing or emerging or volunteer or mandatory incident reporting requirements. The complexity of a reporting environment takes away critical resources from response and recovery actions.

We know threat actors will continue to use recovery events as an opportunity for malicious actions. That is why we are recommending that the Federal Government adopt a single reporting framework. More incident reporting does not equal more security.

Although we have concerns with the cybersecurity infrastructure agency's current version of the Cyber Incident Reporting for Critical Infrastructure Act incident reporting framework, it does offer a single reporting solution.

We also appreciate the work the Office of the National Cyber Director has undertaken to harmonize cybersecurity requirements, as well as Senator Peters' and Senator Lankford's recent proposal the Streamlining Federal Cybersecurity Regulations Act. These are all promising.

Second, information sharing among aviation regulators, the intelligence community, and private stakeholders is foundation to the safety, security, and resiliency of the aviation sector.

Although Federal agencies have made strides to improve information sharing such as multi-agency threat bulletins, information sharing among Federal agencies and width of its aviation sector needs improvement.

The existing information sharing processes lack the speed of relevance and do not consistently validate if existing policies and regulatory requirements are staying ahead of evolving threats.

The airlines look forward to working with the Committee and share cybersecurity challenges, and appreciate the opportunity to discuss our role and involvement, along with recommendations to improve cybersecurity.

Thank you for the opportunity to testify today and I look forward to your questions.

[The prepared statement of General Reynolds follows:]

PREPARED STATEMENT OF MARTY REYNOLDS, BRIGADIER GENERAL, USAF (RETIRED), MANAGING DIRECTOR FOR CYBERSECURITY, AIRLINES FOR AMERICA

Airlines for America (A4A) and our member airlines[1] appreciate the opportunity to testify and discuss the significant emphasis and investment our industry places on addressing cybersecurity challenges in an everchanging cyber threat environment. We thank the Committee for holding this important and timely hearing. There are no "silver bullets" for addressing cybersecurity, but rather, the best, mature cybersecurity programs are risk-based, threat-informed and constantly evolving to stay ahead of a dynamic threat landscape. Our member's cybersecurity programs and investments are based on these foundational principles.

Commitment

Airlines fully recognize that cyber security is one of the greatest challenges facing all critical infrastructure sectors. Airlines continue to make significant investments in information technology (IT) infrastructure and cybersecurity along with consistently partnering with the Federal government and other private sector stakeholders to share information, best practices and lessons learned.

- *Investment:* Airlines take cybersecurity very seriously and are naturally incentivized to invest in their cyber infrastructure to ensure that operations are safe and secure. The safety, security and privacy of passengers and crew are the industry's highest priorities.
  - From 2018–2023, 13 U.S. passenger airlines spent ~$36.5 billion ($6.1 billion per year) on IT, including $7.4 billion in 2023, for IT labor/consulting/equipment/software, to bolster systems resiliency and to make it easier for travelers to shop for tickets and other services; check in for their journeys and navigate airports; check or track bags; modify itineraries; redeem vouchers/loyalty points; and stay apprised of flight status during irregular operations.
  - Airlines' cybersecurity investments include, but are not limited to: identification, prevention, detection, governance, threat and vulnerability management, incident response and recovery.
  - In addition to airlines' full time cyber security employees and other internal resources focused on cybersecurity, airlines use an array of third-party cyber security professionals and contractors, some of whom provide the same services across other industries and government.
  - A4A members invest their time and expertise as critical leaders in developing new and/or updating industry standards. These efforts include improving risk assessments, aircraft cybersecurity and digital information security. In addition, A4A members have created working groups focused on implementing Transportation Security Administration (TSA), Federal Aviation Administration (FAA) and Department of Defense (DoD) regulatory requirements. These working groups also work closely with these regulators to ensure compliance implementation meets the regulatory intent while future requirements are informed by our operator's experiences and recommendations.
- *Information Sharing:* The industry supports and engages in a strong partnership of information sharing with the Federal government and other stakeholders. Specifically, A4A members participate in and contribute to regular and frequent engagement with:
  - The Office of the National Cyber Director (ONCD), Federal Aviation Administration (FAA), Department of Homeland Security (DHS), Transportation Security Administration (TSA), Cybersecurity and Infrastructure Security Agency

[1] *See* A4A's members are: Alaska Air Group, Inc.; American Airlines Group, Inc.; Atlas Air Worldwide Holdings, Inc.; Delta Air Lines, Inc.; FedEx Corp.; Hawaiian Airlines; JetBlue Airways Corp.; Southwest Airlines Co.; United Airlines Holdings, Inc.; and United Parcel Service Co. Air Canada is an associate member.

(CISA), Department of Defense (DoD), law enforcement, the intelligence community and other agencies;

- The Defense Industrial Base, National Defense Transportation Association, Aviation Information Sharing and Analysis Center (A–ISAC), International Air Transport Association (IATA), International Civil Aviation Organization (ICAO), and other cyber-related communities; and
- With the Original Equipment Manufacturers (OEMs) to further understand and prevent possible threats.

A4A airlines are also active members of the A–ISAC mentioned above, involving the senior-most cybersecurity leader for each organization (most often the Chief Information Security Officer (CISO)) and threat intelligence analysts from each organization. The A–ISAC is focused on cybersecurity threat intelligence sharing to help assure the cybersecurity resiliency of the aviation industry. Airlines play a leadership role in A–ISAC and are deeply involved in working groups that address potential enterprise and aircraft vulnerabilities.

Recommendations

Harmonize Federal Requirements: A4A believes that protecting critical infrastructure requires consistent, streamlined and harmonized cybersecurity requirements. As a starting point, we strongly encourage Congress and the Administration to prioritize the harmonization of cybersecurity incident reporting requirements, especially before introducing any new requirements. The current practice of requiring multiple reports to different Federal agencies is a significant and unnecessary burden on industry that reduces the effectiveness of voluntary and mandatory reporting frameworks and increases the likelihood of noncompliance.

- *Existing Cybersecurity Incident Reporting Disharmony:* In the Department of Homeland Security's (DHS) report, *Harmonization of Cyber Incident Reporting to the Federal Government,*[2] the authors identified 45 Federal cybersecurity incident reporting requirements currently in effect. They also identified seven proposed rules, five potential new requirements under consideration and one future rule (*Cyber Incident Reporting for Critical Infrastructure Act* (CIRCIA)). Other than CIRCIA, none of these 58 cyber incident reporting requirements addresses harmonization or contemplates streamlining reporting requirements across Federal agencies.

Although the aviation industry is not subject to all 58 reporting requirements, airlines are currently subject to 10 different Federal departments and agencies existing or proposed, mandatory and voluntary incident reporting frameworks. These Federal agency and department frameworks include:

1. *Federal Aviation Administration (FAA)*—Mandatory Reporting (Advisory Circular 119–1A, "*Aircraft Network Security Program,*" 28 September 2023);
2. *Transportation Security Administration (TSA)*—Mandatory Reporting (Standard Security Program Change, 10 January 2022);
3. *Department of Defense (DoD)*—Mandatory Reporting (Defense Federal Acquisition Regulations Supplement (DFARs) 252.204–7012 and 10 U.S.C. § 391—U.S. Code—Unannotated Title 10. Armed Forces § 391);
4. *U.S. Transportation Command (USTRANSCOM)*—(General Cyber Security Requirements in USTRANSCOM Civil Reserve Aircraft Fleet (CRAF) contract, Appendix 6);
5. *Customs and Border Protection (CBP)*—Mandatory Reporting (Cargo Systems Messaging Service (CSMS) #5285040—"*Reporting a Cybersecurity Event to CBP,*" 12 September 2022 and CSMS #60261003);
6. *Security and Exchange Commission (SEC)*—Mandatory Reporting (*Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies* (In Effect on September 5, 2023)):
7. *Cybersecurity and Infrastructure Security Agency (CISA)*—Voluntary Reporting (*Cybersecurity Information Sharing Act* (CISA) of 2015), pending mandatory reporting (*Cyber Incident Reporting for Critical Infrastructure Act* (CIRCIA) of 2022);
8. *General Services Administration (GSA)*—Mandatory Reporting ((Federal Acquisition Regulations (FAR) subpart 4.4 & 52.204–232, C.F.R part 117) & (32 C.F.R 117.8)).

[2] DHS Congressional Report, *Harmonization of Cyber Incident Reporting to the Federal Government,* September 19, 2023.

9. *Federal Bureau of Investigation (FBI)*—Voluntary Reporting (Report a Crime or Fraud); and
10. *National Aeronautics and Space Administration (NASA)*—Mandatory Reporting ((FAR subpart 4.4 & 52.204–232, C.F.R part 117) & (32 C.F.R 117.8)).

It is important to note that the requirements of these ten Federal agencies differ on definitions, thresholds, processes, timelines, data protections, compliance regimes and content requirements. Although the Federal government probably did not intend to create an environment where 45 cybersecurity incident reporting frameworks with divergent requirements are in effect, it is the environment regulated entities must currently navigate to ensure compliance. For sectors like transportation, with numerous regulators and relationships across sectors, this complex patchwork of disharmonized cybersecurity incident reporting requirements is especially burdensome. Requirements that take critical resources away from identifying, preventing, detecting, responding and recovering from cybersecurity incidents are not the best use of cybersecurity resources.

Finally, harmonization of incident reporting is a good first step, but harmonization of mandatory measures and compliance frameworks are also critically important. A4A supports ONCD's efforts to harmonize cybersecurity requirements across the Federal government. Senator Peters and Senator Lankford's recent proposal, S. 4630, the *Streamlining Federal Cybersecurity Regulations Act,* is also promising, as it would address the challenges associated with multiple regulatory regimes by establishing an interagency Harmonization Committee at the ONCD. Ensuring all mandatory requirements are streamlined and harmonized is in the best interest of regulators and operators, and it will lead to the best outcomes and drive down risk. If harmonization is not possible, then agencies should support a reciprocity framework that reduces unnecessary burdens and allow regulated parties to prioritize critical resources on a threat-based, risk-informed approach.

Improve Information Sharing: Information sharing among aviation regulators, the intelligence community, and private stakeholders is foundational to the safety, security and resiliency of the transportation system aviation subsector. Information sharing is necessary for both:

- Real-time intelligence and information used to protect aviation systems from existing and emerging threats; and
- To inform policy development, verify the effectiveness of policy outcomes, and determine if policy changes are necessary to stay ahead of evolving threats and risks.

However, the existing information sharing processes lack the speed necessary for relevance and do not consistently validate if existing policies and regulatory requirements achieve their desired policy outcomes.

Although Federal agencies have made strides to improve information sharing such as multi-agency threat bulletins, information sharing among Federal agencies and with the aviation sector needs to improve. The information airlines receive from Federal agencies is often not timely or consistent. Additionally, it is not clear processes exist to rapidly update regulatory requirements at a speed necessary to stay ahead of evolving threats. We look forward to continuing to work with aviation regulators, the intelligence community and Congress to improve information sharing.

Conclusion

A4A supports cybersecurity policies and measures that promote a safe, secure and resilient U.S. airline industry and air transportation environment. As cybersecurity becomes increasingly important to aviation safety and security, it requires effective policies, practices and processes, as well as shared, mutual cybersecurity goals among air carriers, Congress and the rest of the Federal government. Critical infrastructure sectors, like aviation, are best positioned when cybersecurity regulations and oversight are consistent and harmonized across the Federal government. The best cybersecurity programs are those that are threat-and risk-based, data-informed, outcome-focused and flexible enough to address evolving threats. Federal cybersecurity policies and measures should likewise share these same principles.

We look forward to working with the Committee on shared cybersecurity challenges and thank you for the opportunity to discuss our role and involvement, along with recommendations to improve our cyber framework.

The CHAIR. Thank you so much. Thank you again to all the witnesses for your testimony.

Mr. Lyttle, you said something in your testimony that just needs a little more emphasis. You are saying our capacity at Sea-Tac is for 30-plus million people and we are at 52 million a year. Is that what you are saying?

Mr. LYTTLE. Yes. We were originally designed for—the current facility is designed for approximately 30 million and we are doing 52 million this year.

The CHAIR. So we are already stretched?

Mr. LYTTLE. Yes, we are.

The CHAIR. And in addition, you are doing construction right now so that is an additional stretch?

Mr. LYTTLE. That complicates it even more, yes.

The CHAIR. Right. So do you think Seattle was specifically targeted?

Mr. LYTTLE. I am not sure why we were targeted. Our understanding Rhysida they have targeted organizations in the USA, outside of the USA, within the aviation industry, but also outside of the aviation industry as well.

The CHAIR. So you do not have any specifics of why you think Sea-Tac was on this particular event singled out?

Mr. LYTTLE. Not at this point.

The CHAIR. OK. And what do you think now? I know you are still in the middle of the investigation and you also do not want to reveal information that might aid and abet others in this particular area.

But is not hygiene a particular aspect of this? We know this from other sectors who have been attacked. Is not the ability for people to attack can come in in all sorts of very easy ways, from phishing and other events? I did not hear anybody talk about this as part of a concern so I just wondered where you were on that issue.

Mr. LYTTLE. Yes, all the—the various different cyber attacks whether it is phishing or whether it is a ransomware attack or a denial of service attack, they are all concerns for us.

We have successfully in the past thwarted denial of service attack, phishing attack. We do—we continuously do exercises. We have internal and external audits that we conduct on a regular basis to minimize the impact of any cyber activity—cyber attacks on our environment.

The CHAIR. So will we learn what exactly happened? Will we at least have access to that information even if——

Mr. LYTTLE. We will be doing—we will be conducting an after action report—independent after action report and that will be available.

The CHAIR. OK. And what is the timing on that?

Mr. LYTTLE. We are not sure as yet. We are focusing on recovery right now and once we have done that then we will conduct the after action report, and we will share this industrywide as well as with the Committee.

The CHAIR. Well, I think to Brigadier General's point that this information sharing is critical, and since so many organizations within our government think that they have a hand in cybersecurity, which they do, this information sharing, kind of, gets lost.

And what we have seen, whether it is other sectors, whether—we mentioned pipelines, casinos got attacked. I remember talking to somebody. The first casino nobody said anything. The second casino—then it leaked out the third casino. They wish they would have known because then they would have taken steps.

So one of the reasons why we wanted to have this today is because we definitely want people to have information about these attacks and what we need to do.

Brigadier General Reynolds, one of the things that we have done is this rulemaking authority through the FAA bill and an ARC, an aviation rulemaking committee, being set up. Does A4A plan to participate in that ARC, yes or no?

General REYNOLDS. Senator, thank you for the question, and yes, absolutely. We are excited that the ARC has been established and look forward to the charter to be released because we would like to participate.

The CHAIR. And what do you think that can do to establishing some sort of focus here on cybersecurity requirements that airports specifically need to look at?

General REYNOLDS. I think anytime there is an opportunity for industry and government to work together to come up with recommendations generally provides the best set of recommendations.

The opportunity to work directly with FAA through this ARC we know can lead to better outcomes and better recommendations. So we are excited. It is the first time we have actually had the opportunity to work in this for cybersecurity specifically so we are looking forward to participation.

The CHAIR. So you are—it is fortuitous that we have this process established?

General REYNOLDS. Yes, ma'am, and thank you again for putting that into the reauthorization. We are looking forward to it.

The CHAIR. OK. Mr. Breyault, you mentioned a lot of things here, and when you think about it the consumer is who we are trying to protect. We are trying to protect our citizens but we are trying to also protect consumers from the impacts of an underinvestment in this particular area. What do you think is most important in that—in the production of the consumer?

Is it at these—the airport in ticketing or do you think that these are leading to individualized attacks, as you said, as that information is then available on the web?

Mr. BREYAULT. Well, Senator, you know, I would say that there are vulnerabilities that impact consumers throughout their interaction with the aviation industry. There are vulnerabilities that impact the safety of the data they provide, for example, to rewards programs or through the frequent flyer miles, through the information they share with TSA when they are—for security purposes, through the actual physical impact that they have when these events happen.

Being stranded at the gate, missing important family events, running through the Sea-Tac airport not knowing which gate you are supposed to go to, are all impacts that happen.

And so I think the cost here really needs to be measured in how do we help consumers recover when these—when these occur because all the investment that I am glad to see A4A and other in-

dustries making in this is not going to prevent all the cyber attacks.

As General Reynolds said, there is no silver bullet and I completely agree with him. So I think what we also need to do, in addition to thinking about how do we prevent the cyber attacks from happening in the first place, how do we create incentives to help consumers recover when they do occur because ultimately they are going to occur and consumers are going to be impacted.

So what do we have in place to help make sure that those harms are mitigated as much as possible.

The CHAIR. Thank you.

Senator Cruz.

Senator CRUZ. Thank you, Madam Chair.

Recently enacted FAA reauthorization includes a subtitle on establishing an FAA Cybersecurity Lead tasked with setting cybersecurity policies and guidance on FAA-regulated aviation operators and avionics.

General Reynolds, how have these provisions in the FAA Reauthorization Act helped to protect the aviation industry from a cyber perspective?

General REYNOLDS. Senator, thank you for that question.

There are a couple things in the reauthorization in particular I would like to highlight. One, of course, is the establishment of the Aviation Cybersecurity Rulemaking Committee. We think that is a very, very good next step.

The second is that inside that reauthorization was a clear callout that the FAA has sole jurisdiction when it comes to rulemaking on cybersecurity around avionics, propellers, and the ground system support systems. Both of those are very, very helpful for us.

It is not just that fact that they have identified them as it is a roles and responsibility issue that goes to harmonization as well.

Senator CRUZ. And how does the Federal Government do abiding by those same standards? In 2022 Congress enacted the Cyber Incident Reporting for Critical Infrastructure Act which generally requires critical infrastructure to report substantial cyber incidents to the Federal Government within 72 hours. A proposed rule is pending that would implement this law.

General Reynolds, do you happen to know how long Federal agencies have to report a major cyber incident to Congress?

General REYNOLDS. Sir, I believe that is seven days.

Senator CRUZ. That is a lot longer than 72 hours that airlines and airports have to report an incident to some of those same agencies.

What about the types of incidents agencies must report to Congress? If an agency suffers a cyberattack what is the number of Americans who, if affected, would automatically trigger a notification requirement?

General REYNOLDS. Senator, if you are talking for the Federal side I believe it is 100,000.

Senator CRUZ. Turning back to the incident reporting requirements for critical infrastructure, depending on the circumstances could the proposed rule require critical infrastructure operators to report a cyber incident that affects only one person?

General REYNOLDS. Yes, sir, and I think the other part I would offer too is that of the 10 different regulatory requirements that we have for incident reporting—some, again, are volunteering, some are mandatory—that the definitions around each are different. The reporting requirements are different. The thresholds are different. Timing is different.

So to say any one specifically is different, they are all different.

Senator CRUZ. Well, that certainly seems inconsistent and potentially overly broad. I should note that my colleagues across the aisle seem to agree. Several of the Democrat authors of law have written comment letters criticizing the excessive breadth of the proposed rule.

The Federal Government is also not much better at securing its networks against cyber attacks. Time and again agencies have been hacked and lost sensitive records on the citizens they are supposed to serve and protect.

Recognizing the regulatory state's proclivity for duplicative regulations without regard to economic burden, Congress included a provision in the cyber incident reporting law to ensure a report to one agency is a report to all agencies.

It also required that agencies take steps to harmonize their cyber incident reporting regulations.

General Reynolds, how is that harmonization effort going today and how many cyber incident reporting regimes is the aviation sector subject to?

General REYNOLDS. Sir, as I meant in the written testimony in our—my opening remarks, it is 10. That is just the number that we have to report to and, again, that is an emerging existing—that is voluntary and mandatory.

In terms of the harmonization I do want to call out at least on one side the FAA, in particular, is using the TSA's requirements in this process. So there is one example where harmonization is in fact happening.

We still believe, though, as CISA continues to work through its comments on CIRCIA we believe that is showing a very good option for a single reporting option for us.

Senator CRUZ. Let us focus on the TSA specifically. What are a few examples of recent cybersecurity directives issued by the TSA?

General REYNOLDS. Sir, somewhat similar to the timeline you talked under the pipeline, we do—we are operating off an emergency amendment. In that side of that amendment there is mandatory reporting. Also in that there is an assessment and then also the development of the implementation plans as well as an assessment plan.

Today we have—our carriers have had their implementation plans approved. We have had the assessment plans reviewed and now we are moving on to the compliance framework.

Senator CRUZ. And has the TSA used notices of proposed rulemaking in advance of issuing these directives to ensure that regulated entities can provide their expert notice and comment on those directives?

General REYNOLDS. I certainly did initially. We did provide comments. I think they felt, and if I had good reason and rationale for

the issuance of emergency amendment in that process there is not the opportunity to provide comments.

So we have been working very closely with them. We have a good working relationship with TSA. We work with them to make sure we understand our compliance requirements and they ask and work with us to make sure they understand how we do threat-based risk-informed programs so that their compliance program actually complements what we are doing today.

Senator CRUZ. The Cybersecurity and Infrastructure Security Agency, or CISA at DHS—the same CISA that works with the FBI to pressure social media companies into censoring conservatives—is in charge of implementing this legislation with the national cyber director.

So we should not be entirely surprised that the Biden-Harris administration has failed to implement the legislation in a measured and reasonable way.

What can be done to simplify and harmonize the various regulatory burdens being placed upon aviation?

General REYNOLDS. Sir, I think, first, I would just pick incident reporting. I mean, 10 seems like it is too many.

So if we can find a single reporting framework that can be adopted by all Federal agencies and departments and that department can then take the information, consolidate and analyze it, and get it out to not just other Federal agencies but also to the private sector—critical instructor sectors—we would all be in a better position.

The last thing I think anyone would want to do during a recovery and response issue is having to worry about going through a compliance matrix and figuring out which time, where do I have to report, different elements.

And I do not think the Federal Government's response would be any better if you get 10 different agencies receiving information at different times at different periods.

Senator CRUZ. Thank you.

The CHAIR. Thank you.

Senator Hickenlooper, I think we got you in under the clock. I know you have to preside at 11 so——

STATEMENT OF HON. JOHN HICKENLOOPER, U.S. SENATOR FROM COLORADO

Senator HICKENLOOPER. I appreciate that. Thank you, Madam Chair, and thank all of you for your—for being here today and your public service on these issues.

Mr. Breyault, ransomware attackers often attempt to shut down computer systems and steal confidential data that they can extort businesses or individuals somehow, get—well, basically stealing the data and trying to sell it. Consuming—keeping consumers' data secure, making sure that we do not collect excessive and unnecessary data also helps reduce risks from financial fraud and scams while, again, protecting people's privacy.

What proactive steps, Mr. Breyault, can businesses take to protect their customers' and employees' sensitive and personal data?

Mr. BREYAULT. Senator, thank you for the question. I am not an expert on what businesses themselves should do, specifically what

tools they should implement, but I know that there are strategies that agencies like the Federal Trade Commission have in advice they have provided to those businesses, and I think you alluded to a few of them.

Number one, it is doing an inventory of what information you are actually collecting to find out where you—and then to find out do you actually need that information to conduct the business, and if you do not need that information can you minimize the amount of data that you are holding on to.

If you are reducing the threat vector, the number of places—number of bases you have to cover, to use a baseball term, it is easier to play defense against the cyber thieves.

Then knowing how to get rid of that data securely, get rid of data that you are taking in as part of your business securely, and then finally having a recovery plan in place when all those other things you have done do not work so that consumers, at the end of the day, can be as—can help to—your customers can recover from that.

Senator HICKENLOOPER. Sounds like sound principles to me.

Mr. Reynolds, cyber attackers attempt to cause disruption in order to create urgency for victims to pay ransom. A quick recovery is in the interest of the business and the interest of its customers. Also reduces the leverage that attackers use to try and extort their victims.

As we have seen in some notable cybersecurity incidents it can take weeks or months for impacted organizations to fully recover.

In addition to what—excuse me, in addition to what Mr. Breyault was describing, can you describe what steps your member companies take to prepare and practice recovering from cyber attacks as part of their cyber resilience? So not necessarily the preparation but the recovery.

General REYNOLDS. Senator, thank you for that question.

I think I will start with our North Star which is we always keep safety, security, and privacy of our customers at forefront. Our programs are risk-based threat informed. They have to evolve with the threat.

Some of the things that we do in terms of coming up with ways in which we can improve are things like tabletop exercises—policies and programs and training. One example I might have is that although we do tabletop exercises and exercises and planning internal to each of our companies, at the industry level we also work with the Federal Government.

So there is—in fact, this week at a conference the Aviation Information Sharing and Analysis Center is conducting a global exercise where they bring in Federal regulators and the airlines and airports to work through a very comprehensive exercise so that we can all learn.

We can get a report from that. We can look at gaps and seams so we can all improve. We have done the same thing with the FAA recently.

They have the Aviation Cyber Initiative that we participate. We took six months to actually build out a program with them and participated in an exercise with them. It is a comprehensive program, sir.

Senator HICKENLOOPER. Great. I appreciate that.

Mr. Lyttle, a very sobering event that you had to go through. Just so far, what lessons would you want to share with other airports in terms of things that could be useful? Lessons learned?

Mr. LYTTLE. Some lessons learned as was just mentioned, for example, is to actually go through and do tabletop exercises.

We were fortunate that we actually did a tabletop exercise which simulated a ransomware attack in the past. I can tell you in reality it is a whole lot more complicated but it actually helped.

Also having continuity of operations, code plans in place. Every department at the port is required to have a code plan and we have to activate those really fast. Also, to practice your NIMS and activate an incident command, emergency management policy rooms, practicing that over and over again and then partnering with, of course, the Federal agencies such as CISA, the TSA, and also outside subject matter experts and conduct various different—like ethical hacking. Do that on a regular basis to test and test your environment.

Senator HICKENLOOPER. Well, I am out of time. But I do think at some point it also would be worth looking at are you collecting—are you getting rid of data that is no longer necessary? In other words, saving data and therefore making yourselves or your consumers a target?

Mr. LYTTLE. Yes. My recommendation if you do not have to store sensitive data do not but if you have to ensure that it is encrypted.

Senator HICKENLOOPER. Fair enough. Thank you.

Thank you, Madam Chair.

The CHAIR. Thank you. Thank you.

Senator Blackburn.

STATEMENT OF HON. MARSHA BLACKBURN, U.S. SENATOR FROM TENNESSEE

Senator BLACKBURN. Thank you, Madam Chair, and thank you all for the hearing today. We appreciate that.

Mr. Reynolds, I want to come to you first and talk about the known crew member program. One of the things that has come to our attention is the abuses there. I know earlier this year four flight attendants allegedly smuggled millions of dollars in drug money out of the U.S. using that known crew member lane at JFK Airport.

We have also learned that two hackers discovered a vulnerability in the system that allowed them to create profiles for fake employees and this was giving them access to areas beyond the security checkpoint.

So what efforts are you taking to make certain that this is secured?

General REYNOLDS. Senator, thank you for that question.

The known crew member program is not something that I personally deal with particularly. That is not my area of expertise.

I will say, though, the program is among—is actually is among key stakeholders including TSA, A4A, and ALPA. It is a program to help facilitate screening a trusted population of airline crews and it involves close collaboration to ensure the cybersecurity of those systems.

Because I am not the expert in that, ma'am, I would love to take your question back and actually talk to our leads and provide you a more comprehensive—I want to make sure my answer is correct.

Senator BLACKBURN. I would appreciate that. I think that is something that is important to each of us, especially when you look at the issues that are in this country with the drug trafficking and the cartels, and that is a point of concern and, indeed, vulnerability.

But then to find out that hackers have found a way to get in and create these fake profiles, I would like to have some more information on that and then be able to decide if there are other actions that we should take.

You all talked a minute earlier about information sharing, and as we look at 2030 when there are going to be 32.1 billion devices connected to the Internet here in the U.S. I think that this is going to need more attention when you look at that timeliness and the importance of streamlining reporting requirements and streamlining how you increase this information share.

So you have made a couple of comments but I want you to drill down a bit on what you would do with the streamlining process?

General REYNOLDS. Senator, thank you. To talk on the information sharing piece of it, our threat risk based programs are—information sharing is absolutely critical to it and when we talk information sharing there is two elements, I think, that are important to make a distinction about.

There is the information sharing that is necessary to protect your networks with what the adversary is trying to do immediately, like, within a short order. Whether that is tactics, techniques, and procedures, it is incidents of—or a compromise, it is that kind of level of detail that you know that your program is either safe or you have to make corrections.

There is a second part of the information sharing that I want to highlight, too, and that is that same kind of level of information, how is it being used and can it be used to inform requirements—policy requirements and regulatory requirements to make sure they stay ahead of the evolving threat landscape.

So those two pieces we would love to see those actually improve and, in fact, bring in more industry input so that we can assure that the information shared not just among and across is an example.

I just want to call out the Sea-Tac team because they did an amazing job of pulling industry together so that we can understand what was happening not just operationally but from a cybersecurity perspective they were able to share techniques procedures.

They were able to tell us who they think the actor was and that way we can go back to our own networks and make sure they were protected.

Senator BLACKBURN. Well, and we also think workforce is an important component of this and we—Senator Rosen and I have a bill that would work on training that workforce.

I am just about out of time so I am not going to—I do have a question for Mr. Lyttle. I am going to submit this because when it comes to ransomware and the demands that are there and, of

course, the targeting that you all went through we think that the relationships with public and private partners are very important, and I will submit that question to you for a written response.

Thank you, Madam Chairman.

The CHAIR. Thank you, Senator Blackburn.

Senator Klobuchar.

STATEMENT OF HON. AMY KLOBUCHAR,
U.S. SENATOR FROM MINNESOTA

Senator KLOBUCHAR. Thank you very much, Madam Chair. Thanks for doing this important hearing.

So the recent CrowdStrike outage we all know plagued our airports, plagued our transportation, and it was caused, as we all know, by a flaw in this security update.

Mr. Breyault, in your testimony you highlight the growing trend in ransomware attacks in the aviation center. Can you speak to how investing in secure interoperable networks can protect consumers while something else was going on here with CrowdStrike?

Mr. BREYAULT. Senator, thank you for the question. I would respond to that by saying that more investment in cybersecurity resiliency will help address not only the ability of aviation networks to resist hacking, but it would also give them resources to help train the staff who interact with those networks.

I think as most experts in cybersecurity will tell you, humans are often the weakest link in any cybersecurity chain. And so Chair Cantwell talked earlier about the need for greater hygiene to get staff and other people who interact with these networks to avoid things like clicking on suspicious links that can subject an entire network to a ransomware attack that ultimately shuts it down and has these dramatic impacts on consumers—the missed flights and things that I talked about.

I think one thing that has not come up yet that would, I think, also play a role into this is the emerging threat of AI. We are very concerned at NCL that the bar to entry for cyber thieves to conduct these ransomware attacks is really going to be dramatically lowered because of the ability of AI to make it easier for people who may not have the same skillset that you may have needed five or 10 years ago to commit a ransomware attack to commit one.

So the number of threat actors out there we fear is only going to multiply and so the kind of investment that we need in cybersecurity resiliency is more urgent now than ever.

Senator KLOBUCHAR. And, Brigadier General, what additional tools and skills will our current cybersecurity workforce need to be able to deal with this?

General REYNOLDS. Senator, thank you for that question.

As you point out, there is certainly a shortage of IT professionals in this country. One of the things from the aviation perspective that we work very closely on is that it is hard to find IT professionals that have both IT experience and aviation experience.

So in many cases we have to bring them—bring folks in and we provide them that additional training so they understand the specifics of aviation IT.

And that would be one thing I would say that for companies that are looking for folks to populate their team is that you have to

think about how do you internally train these folks—how do you actually bring them on board and actually provide them the necessary skills to not just stay ahead but understand the industry they are participating in.

Senator KLOBUCHAR. Mmm-hmm. And just a last question, Mr. Lyttle, just on the same topic. In your testimony you note how Federal agencies like Cybersecurity and Infrastructure Security Agency have helped the Seattle Airport improve workforce development.

I think we have got 464,000 unfilled cybersecurity jobs in the U.S. One in three of those unfilled jobs are in the Federal Government.

Tell me what you think the Federal Government should do to get those numbers to be in a much better place?

Mr. LYTTLE. So—well, we can pay people more, but one of the things I think we can do is we have to attract expertise pretty much before they start going to college, start getting them interested in the aviation industry so they see aviation as a career, and so they can start deciding on an aviation career before they decide to go to some other industry.

Senator KLOBUCHAR. Mmm-hmm. OK. Very good. Thank you very much. Thank you, Chair.

The CHAIR. Thank you, Senator Klobuchar.

Senator Budd.

STATEMENT OF HON. TED BUDD,
U.S. SENATOR FROM NORTH CAROLINA

Senator BUDD. Thank you, Chair. And, again, I thank the panel for being here.

I want to talk about a different type of attack. It is an electronic attack, particularly GPS spoofing, which is increasingly impacting commercial and GA aircraft.

I have had pilots send me photos of panels at 43,000 feet with a terrain warning. There is no terrain at 43,000 feet, particularly flying in the Middle East or overseas.

Now, in the FAA Reauthorization Act of 2024 it does have provisions to secure aircraft electronics against these sort of attacks. But there is additional—but my question is this, particularly General Reynolds.

Are there additional actions that Congress or the Executive Branch should take to address this growing issue?

General REYNOLDS. Senator, thank you for the question.

I think the piece I might offer is maybe talk a little bit about what we are doing right now with the Federal Government that might help think about what kind of initiatives or resources might be beneficial to go after this problem.

One is the FAA does a great job of actually highlighting where those interference patterns are actually happening. If you look at a globe it is pretty extensive in the places you would expect around the Ukraine area and the Middle East.

Having that kind of awareness before we actually fly into these locations is absolutely critical. The second is that we are working with the Aviation Cyber Initiative. As they develop a concept of operation, so if pilots do, in fact, fly into an area—the examples you just provided—they have the processes that they can—they actu-

ally identify the issue and know where to report it and then once the reports are actually made then what can the FAA and others do to actually notify others and do mitigation if that is possible. In fact, it might part of that be contacting law enforcement.

And then last, just recently I mentioned that we are doing with the ACI or the Aviation Cyber Initiative—we just had a tabletop exercise on this very subject and in that we were trying to identify gaps and seams, communication breakdowns.

And I think to your question, sir, as those initiatives continue to evolve I think it would be well worth the time to talk with the FAA to see what resources they need to actually help all of us.

Senator BUDD. Very good. Thank you. I yield the time.

The CHAIR. Thank you. Senator Duckworth.

Thank you for your leadership on the Subcommittee.

STATEMENT OF HON. TAMMY DUCKWORTH,
U.S. SENATOR FROM ILLINOIS

Senator DUCKWORTH. Thank you, Madam Chair, and thank you for holding today's hearing. The recent Sea-Tac cyber attacks on Sea-Tac is a real chilling reminder of the grave and growing risk to our Nation's aviation system in cyberspace.

These types of cyber attacks are serious crimes with serious implications that go far beyond mere passenger inconvenience. The source of the attacks—these most recent attacks, the Rhysida ransomware is an entity that is rumored to be based in Russia or within its sphere of influence.

Rhysida has been associated with attacks on the British Library as well as government institutions in Portugal, Chile, and Kuwait. It has also claimed responsibility for an attack on Prospect Medical Holdings here in the U.S. and this raises questions about national security.

This is also not the first time a United States airport has been attacked and in 2022 a pro-Russian hacker group that called itself Killnet orchestrated an attack on a dozen U.S. airports, including, LAX, Atlanta, LaGuardia, and both of the airports in Chicago, O'Hare and Midway.

And while, thankfully, the 2022 attack did not disrupt operations we cannot count on that always being the case. Attackers also target sensitive personal information.

The cyber criminals behind the Sea-Tac attack recently posted a ransom demand of almost $6 million in which they threatened to sell stolen PII like scanned U.S. passports and forms with our Social Security numbers.

Worldwide, aviation cyber attacks increased 24 percent in the first half of 2023 and they are ongoing, and just in the last 30 days the City of Chicago's flychicago.com website blocked 1.09 million malicious site requests.

Mr. Lyttle, what more should the Federal Government be doing to help airports harden their cybersecurity to protect against threats from foreign actors?

Mr. LYTTLE. Senator, the aviation industry is required, for example, to submit the CIPs that was mentioned and the assessment plan—security improvement plans and assessment plans, and all airports are required to submit this.

One way that we could help is if the TSA and CISA consolidate this information, comes up with best practices, and actually disseminate it back to the aviation industry. Currently, it is a one-way street that we are sending the information but we are not getting back in a timely enough manner recommendations of how to improve our infrastructure. That would make a major difference.

Senator DUCKWORTH. Thank you.

General Reynolds, I thank you for your service and I could not agree with you more about the challenges of finding IT professionals who both know cyber and also aviation. What more should the Federal Government be doing to help airlines harden their cybersecurity to protect against threats from foreign actors, especially since so many of them are—get maintenance overseas as well?

General REYNOLDS. Senator, thank you, and thank you for your service as well. Thank you.

I think I will start with the two points I made earlier, which is first on harmonization the fewer incident reporting requirements that we have the better for us so we do not spend all our time worrying about compliance and, more importantly, we want to make sure the information is going to the right places at the right time.

The second part is on the information sharing, improving information sharing not just amongst ourselves in the industry side but amongst the Federal agencies and with each other.

The better we can do that at the speed of relevance the better we are all going to be. Our programs rely on making sure we can stay ahead of the threat actors and that information sharing is key to it.

Senator DUCKWORTH. Are there any additional vulnerabilities with foreign national airlines? So, you know, because there are accessing our systems in partnerships with American Airlines, the Star Alliance and all of these other alliances. Are there vulnerabilities there?

General REYNOLDS. Ma'am, I would not want to talk—if there were I would not want to talk about the vulnerability specifically, but I will say our programs are threat based in risk informed, which means we do the analysis on—anytime a system is connected or we share data one amongst one another we do that analysis to make sure the threats are known and they are minimized, in fact, to the zero point if we can.

I do not—I am not an expert on the international carriers and what their exact systems are and the vulnerabilities, and I can certainly circle back and provide more information for you.

Senator DUCKWORTH. Thank you. Thank you.

I am a pilot myself and I know that, you know, the basic thing in aviation safety is you should never be left to a single point of failure in any aviation system and that redundancy saves lives.

When Boeing left a safety critical system—a safety critical system on the 737 Max dependent on single angle of attack sensor two flights crashed, killing 346 people.

So when I see the NOTAM system knocked out by an accidental file deletion and so much of the aviation system knocked out by a CrowdStrike software update that really worries me. That is a single point of failure and we do not want that.

So to protect—better protect our aviation systems from cyber attacks I believe we need to improve both redundancy and resiliency and each of you have spoken to this.

But, Mr. Lyttle, I just want to give you a little more time. How can airports, airlines, and the Federal Government work better together to help improve the redundancy and the resiliency in our aviation system's computer networks?

Mr. LYTTLE. Yes, I think we have to do far more information sharing. We can always learn from each other. Airports can learn from other airports and we can also learn from the TSA and CISA in terms of information that they are gathering and threats that they are seeing out there, and share this information immediately with the aviation industry.

Airports in general have very robust cybersecurity but nothing is impenetrable. Nothing is 100 percent secure. So if we can actually learn—each airport can learn from each other and I think the consolidation point TSA because we are required to submit all of these plans to the TSA and to CISA, I think if they consolidate this information, come up with a recommendation in standards in a much more timely manner and disseminate back that to the aviation industry so that we can continuously improve our cybersecurity defenses I think that would go a long way.

Senator DUCKWORTH. Thank you. I yield back.

The CHAIR. Thank you. Senator Schmitt.

STATEMENT OF HON. ERIC SCHMITT,
U.S. SENATOR FROM MISSOURI

Senator SCHMITT. Thank you, Madam Chair.

I did have a couple of questions but first I wanted to sort of make a statement here. As our aviation sector becomes more reliant on modern network solutions the need for stronger, more resilient operating systems grows to protect against malign influences both foreign and domestic.

Today, we face a rapidly changing threat landscape. Cyber attacks against airports and airlines are growing and becoming more sophisticated.

Whether it is a breach of sensitive data, disruptions to critical operations, or ransomware attacks that cripple entire systems, these threats have the potential to cause widespread disruption.

While I do not disagree with the emphasis of this hearing today, I believe that we also must draw attention to self-inflicted wounds and failures experienced by our Nation's aviation system and the national airspace and international airspace under President Biden and Secretary Buttigieg's leadership.

In January 2023 the United States experienced its first nationwide ground stop since 9/11. This was the result of an input error to the notice—to air emissions NOTAM system by an FAA contractor, causing the entire NOTAM system to crash.

As a result, thousands of flights were delayed and/or canceled, stranding hundreds of thousands of passengers across airports across our country.

One of the Biden administration's first actions under the leadership of Secretary Buttigieg was to change the name of the NOTAM

system from the notice to airmen to notices to air mission to be more inclusive.

Americans who are flying want to know that their systems are safe and reliable, not whether or not—whether or not if we name our systems to be more inclusive or not. This is a consistent lack of leadership and priorities from this administration. It is way more focused on virtue signaling than actually safety.

Additionally, late last year cybersecurity firm CrowdStrike implemented a faulty software upgrade it deployed to Microsoft Windows customers, crippling airline operations in the United States that led to nearly 3,000 flights being canceled in one day.

Delta Airlines in particular canceled nearly 7,000 flights and faced issues for weeks from the software update failure. I make no mention of the increased number of near misses, mass cancelations and issues faced by Southwest during the 2022 holiday season.

Unfortunately, Secretary Buttigieg has shown blind willingness to prioritize woke ideology that values social cultural merits over safety. I say all of this to validate that it is no coincidence that our aviation system faces its biggest inflection point right now.

The American flying public deserves better leadership, and as I have stated over and over this administration has failed time and time again and, by the way, Secretary Buttigieg has not been in front of this committee in the two years that I have served on it.

Mr. Breyault, I do have a question that—I do not think this has been asked yet but, you know, TSA is in the process of deploying more biometric technologies at airports and at security checkpoints.

If there is a cyberattack would—how vulnerable is that data to hackers? This is one of these things that we do not talk about much up here but people back home it is a question that they will ask me is if they are signing up for Clear or something like how vulnerable is that very personal data?

Mr. BREYAULT. So, Senator, thank you for the question. There is no 100 percent solution in cybersecurity and that would also apply to the biometric data that a consumer might share with TSA or as part of Clear.

And so I think that what that means is that each consumer has to do their own risk analysis on I am giving over for me personally, and this is speaking for me, I do not sign up for Clear for those specific reasons, because I am unaware of how well they are protecting that data and something like biometrics is—you know, I cannot change my fingerprint. I cannot change my face.

That is a unique, persistent identifier of me, and while there may be good reasons to use that and I think an argument can be made that biometrics can help prevent people from spoofing who I am and getting through TSA—I think Senator Blackburn was alluding to this in a question she had earlier—I do think there are legitimate concerns that consumers have.

And so I think it is incumbent on all entities, including government agencies like TSA that collect consumers' information, particularly the sensitive personal information, and I think biometrics has among the highest levels of sensitivity to protect that because in the wrong hands it can be used for harm.

Senator SCHMITT. Thank you. Thank you, Madam Chair.

The CHAIR. Thank you.

Senator Welch and then Senator Rosen.

STATEMENT OF HON. PETER WELCH,
U.S. SENATOR FROM VERMONT

Senator WELCH. Thank you very much. I was going to ask Lance Lyttle a question about what happened at Sea-Tac. First of all, my understanding is that Sea-Tac had some backup information or had backup access so that it was not—that mitigated significantly the cyber attack. Is that right?

Mr. LYTTLE. Yes, we did have backup and the backup was not compromised.

Senator WELCH. Yes. Well, that is terrific. Thanks for that. Just one question. On the passengers were they all able to get everything that they had lost—baggage and so on?

Mr. LYTTLE. So in the—when we just started because we had to shut basically the systems down so we could prevent any further attacks we had to actually execute or a continuity of operations plan and one of them is actually to start doing—sorting bags manually.

We also had to implement what we call a fallback tag where we do a semi-manual process with bag tags because the system that the airlines used to actually access the bag tag information that system was inaccessible. So we had our backup—two backup plans that we actually used to go through that process until we actually restored access to what we call the bag sortation messaging system.

Senator WELCH. How long did that take before folks got their bags back?

Mr. LYTTLE. It depends. For the—it varied for the different airlines. So for I think Alaska and Delta we got that back in two days and then for the other airlines it took us a little bit longer.

Senator WELCH. Thank you.

You know, the other thing in that hack a lot of individuals had their private information compromised or could be compromised and the question I think I have for you but it also would apply if this happens again, and obviously there are bad actors out there that are hoping or trying to make it happen again, is there monitoring on behalf of those folks whose information may have been compromised so that if it is used they are given that information? That is something that was provided after the OPM hack in the government.

Mr. LYTTLE. Yes. So any employee that we find that their personal information has been compromised we are going to notify them immediately and we are going to provide credit monitoring as well.

Senator WELCH. So you are actively doing that?

Mr. LYTTLE. Yes.

Senator WELCH. You will know if there is one of your employees that has had his or her information compromised you would be able to alert that person?

Mr. LYTTLE. Yes, we will alert them immediately and we will provide credit monitoring and other—any other support services.

Senator WELCH. And I am not sure how much information about this hack you have decided Sea-Tac has provided, but is it com-

mitted to sharing more details and the lessons learned as more information becomes available?

Mr. LYTTLE. Yes, definitely. Just immediately when the incident happened we actually facilitated—a call was facilitated through Airport Council International where we got all the airlines—sorry, the airports and some airlines together just to let them know exactly what was happening so they could take actions to prevent it from happening there as well.

In addition, we are going to conduct the after action report that is going to be done by a third party vendor and we will share that information industrywide so everybody can utilize it to improve their cyber defenses as well.

Senator WELCH. All right. Thank you very much.

And for Marty Reynolds, have the—all the flying passengers who were impacted by the CrowdStrike outage been adequately and fairly reimbursed for their travel?

General REYNOLDS. Sir, thank you for that question.

My expertise is in cybersecurity and it is not in accommodations, and I want to make sure I get you the right answer and an accurate answer to your question. So I would like to take that back and provide you an answer.

Senator WELCH. Well, I would like it if you would do that. I appreciate that.

And let me ask John Breyault from the Consumers League, you know, when I fly a lot of folks around me are using the Internet and what is the security situation with respect to Wi-Fi in flight?

Mr. BREYAULT. Senator, thank you for the question. While I cannot speak to sort of specific security tools that airlines implement for their in-flight Wi-Fi what our general advice to consumers is whenever they are using a public Wi-Fi network, and I think this would definitely apply when you are on an airplane, is to avoid sharing sensitive information.

So, for example, if you are—I would advise against doing things like online banking, for example, if you are on a public Wi-Fi network because you just do not know who may be snooping on that signal.

So, you know, I think that generally applies to in-flight Wi-Fi, though I would be happy to see what I can find and get back to you about sort of if there were specific security protocols.

Senator WELCH. Yes, I would like that. So you are suggesting that folks who are using in-flight Wi-Fi take precautions as they would potentially in any public access Wi-Fi situation?

Mr. BREYAULT. Yes, Senator.

Senator WELCH. Thank you. I yield back.

The CHAIR. Thank you. I am so glad our colleagues are showing up for this important hearing. I do not know if you are ready or not, Senator Capito.

And Senator Rosen has been on the screen for some time but I know, Senator Peters, you were next. Would you be willing maybe to defer to Senator Rosen?

Senator PETERS. I would be happy to defer to Senator Rosen.

The CHAIR. OK. Senator Rosen.

STATEMENT OF HON. JACKY ROSEN,
U.S. SENATOR FROM NEVADA

Senator ROSEN. Thank you so much, Senator Peters, and thank you, Chair Cantwell, I really appreciate that, and really appreciate you holding this important hearing on supporting airports and airlines against cyber attacks like the ones that took place in Seattle-Tacoma International Airport.

You know, travel and tourism I do not have to tell anyone they are the backbone of Nevada's economy. Our airports are the gateway to everything we have to offer in Nevada. So we have to do everything in our power to protect them along with heliports, air traffic control systems and aircrafts.

Together, this really is critical infrastructure and this critical infrastructure faces complex and ever changing cybersecurity threats and challenges that we must work together to address and mitigate.

And so, Mr. Lyttle, talk a little bit about network segmentation because in the wake of the cyber attack on your airport you said tools ranging and networks ranging from employee e-mail to passenger information systems and public Wi-Fi all became unavailable.

So one of the first actions taken in response by the Port of Seattle was to isolate critical systems. However, basic cyber hygiene recommends that networks should already be segmented in a way that separates critical services including the separation of public and internal systems.

And so, Mr. Lyttle, I know Senator Welch talked about this a little bit but in what ways were critical systems at the airport connected to public systems? So you have critical systems.

Were they connected to external websites? Were they connected to public Wi-Fi whereby ransomware could really gain access to them and impact all of these systems at once? Are they segmented in such a way?

Mr. LYTTLE. Yes. Thanks for the question, Senator.

One of the reasons why we were able to recover so quickly or to have some of our services not interrupted is actually because we have segmentation.

So, for example, our access control system was on a totally segmented network. Our conveyor systems were on a totally different network. So the network that was actually impacted again was segmented.

That is something that we have been doing for years and one of the lessons learned is we will actually do actually more segmentation. But there are several systems at the airport that was not impacted because of segmentation.

Senator ROSEN. Fantastic. I want to build on that with General Reynolds because we have airline networks and we know they interact with airport systems—airlines and airports. That is how you update a lot of information, right?

So how vulnerable is this interoperability between the airlines and the airport systems in the event of a cyber attack? How do you segment or mitigate this threat as airport—as airlines and airports talk to each other? Of course, in this case we will just use this for an example, getting your bags.

General REYNOLDS. Senator, thank you for the question.

As I stated upfront, our programs are mature programs. They are risk based threat informed, which means we follow standard practices. For example, the cybersecurity framework that NIST puts out is one of the foundational principles that we follow—the standards that we follow.

One of the things you do in those circumstances that you identify your systems and then prioritize those that are critical—less critical, and then the identification you look for those connections you are talking about and those connections you are then looking to see what controls can I put around those areas to minimize the risk that you may have when you connect systems to one another.

Senator ROSEN. That is great, because I want to bring up something really important while you talk about connecting systems to mitigate risk because we have third-party vendor cybersecurity issues, potentially.

Last month cybersecurity researchers found vulnerabilities in a tool that supports the known crew member program which allows pilots and crew members to pass through TSA without screening—without screening.

So, General Reynolds, to provide guidance to member airlines to ensure that they are doing their due cyber diligence with vendors this intersects with airlines.

It intersects with our security—our personal security, our homeland security—and would it be better to have all the airport crew—maybe they have their own lane but they use the same kinds of identification that we use every day when we go through TSA?

General REYNOLDS. Senator, thanks for that question. It is a good question. I will say my expertise is not the known crew member program. That is not where I—that is not where my expertise is at.

I will say we are happy to take your question back to those of the program leads——

Senator ROSEN. Thank you.

General REYNOLDS.—and try to get you better information.

Senator ROSEN. Thank you. I sure appreciate that.

And Senator Cantwell, thank you again. Senator Peters, I yield back.

The CHAIR. Well, thank you, Senator Rosen.

It takes a COBOL programmer to ask some really tough questions here of the witnesses. So thank you for that.

[Laughter.]

The CHAIR. I think it is important, these issues on interopabilities and vulnerabilities because I think that is what we are really talking about today. The most vulnerable—we are only as strong as our most weak link and that is what you are articulating there. So thank you.

Senator Capito, followed by Senator Peters.

STATEMENT OF HON. SHELLEY MOORE CAPITO, U.S. SENATOR FROM WEST VIRGINIA

Senator CAPITO. Thank you, Madam Chair. Thank you, and thank you all for being here today.

General Reynolds, I want to start with you. Cybersecurity insurance is becoming increasingly important across the country and across our economy and, certainly, for the aviation sector.

Senator Hickenlooper and I have a bill, the Ensure Cybersecurity Act, which would help create a working group of experts to look at different ways to improve understanding and to share information so that potential customers are better equipped to make better decisions.

Do you think this bill would be beneficial? I am not certain that you know exactly but also what kind of challenges are airlines facing looking at trying to secure cybersecurity insurance?

General REYNOLDS. Thank you, Senator, and cyber insurance it is complex and it is always evolving. I think that is probably the place I would start is it—when you have your policy and you move from one incident to another incident working with your insurance provider you want to make sure you fully understand what is covered and not covered.

Any new proposals you have mentioned—and I am not as familiar with your proposal—but if a working group and it can be established and it can provide clarity in that space then I think we would certainly welcome it.

Senator CAPITO. Yes. Thank you. You also mentioned in your testimony that airlines have to report to 10 different agencies with 10 different timelines and other reporting requirements. It seems incredibly burdensome but we want to ensure safety, obviously, first as you do or kind of a siloing of information.

Do you have concerns that reporting on all these different agencies on different timelines poses a greater security risk because of the varieties or do you think it provides more security?

General REYNOLDS. Ma'am, I am not sure it would provide greater security. I do know that in those incidents—and we have not fully exercised it, thankfully. We have not fully had to fully exercise and report to all 10.

But what I would suggest is that in the time that you are trying to identify and recover from an incident the last thing you want to do is have to repeat the reporting and report on different kinds of definitions, thresholds. Data protections are different.

So it is not beneficial. Let me just put it that way.

Senator CAPITO. Yes, it is burdensome and probably less efficient and——

General REYNOLDS. All of the above, ma'am.

Senator CAPITO. All of the above. I could go on and on, I guess.

Mr. Lyttle, I understand that you decided not to pay the ransom—I am sorry I missed the testimony—but you decided not to pay the ransom and you mentioned that if any personal information is compromised you are going to notify them and provide support from your—the wake up call that you had at your airport.

Let me ask you this. You are the eleventh busiest airport, right, in the nation?

Mr. LYTTLE. Currently.

Senator CAPITO. And my airport in my capital city is the one hundred and eighty-ninth and this sort of goes to what the Chairwoman was just talking about in that you are only as secure as your weakest link.

So all of our airports but the smaller airports are just as vulnerable to these kinds of attacks and could get people into systems that could have impacts in all of our systems.

What kind of perspective can you provide having had this experience?

Mr. LYTTLE. With regards to paying the ransom, which that was contrary to our values and we do not think it is the best use of public funds, so we decided not to pay.

Information sharing, I think, is extremely important. Whereas our airport being a much bigger airport we have more resources, a smaller airport such as yours probably does not but they can actually learn a lot from what we are doing and benefit from what we are doing rather than starting from scratch to—you know, to figure out how to improve their cyber defenses here we have gone through this experience right now and even though we had a lot of resiliency in place, continue to have operations plans in place, we are going to learn a whole lot from this experience as we conduct our after action report.

And I think sharing this information with large, medium, and small airports is going to be beneficial to the entire industry, not just with airports but also with airlines as well.

Senator CAPITO. Right. So under Homeland Security we have an organization that is chaired by Jen Easterling, which is the CISA—it is the Critical Infrastructure for Cybersecurity—and they bring best practices around.

I am sure that you have talked—your organization has talked with them to report your incident so it could help other airports as we move forward.

So I want to put a little plug in for Marshall University in my home state of West Virginia—is creating Cybersecurity Institute for Critical Infrastructure of which aviation is a part. We think of it—you know, we think of it finance and military and defense.

But if somebody knocks out our critical infrastructure, as we found out in certain instances for one thing or another, we are as vulnerable and maybe in some ways more vulnerable—food supply, et cetera.

So what—the point of this institute is to create a workforce that can then meet the cybersecurity challenges of the future in our critical infrastructure space.

So I may reach—have my folks reach out to you to find your experience and that might be useful to them as they are creating the curriculum for the cybersecurity workforce of the future.

And I appreciate you all.

Mr. LYTTLE. Happy to participate.

Senator CAPITO. Thank you.

The CHAIR. Senator Peters, thank you for your indulgence. Very much appreciate it. But so happy to have you here because of your role in the Homeland Security Committee and this committee, too. So thanks for your leadership.

STATEMENT OF HON. GARY PETERS,
U.S. SENATOR FROM MICHIGAN

Senator PETERS. Well, thank you, Madam Chair. It is great to be here and thank you to each of our witnesses for your testimony here today on an incredibly important issue.

Mr. Lyttle, you have been testifying here today and thank you for your very detailed testimony and the work that you have engaged in to combat the extremely concerning incident that occurred at Sea-Tac.

And although this hearing has been focused on cybersecurity and aviation it certainly shows that this attack also highlights, I think, other cybersecurity attacks including our ports—our maritime ports.

Michigan is the home to 33 active cargo ports that ship or receive cargo. They handle 51 million tons of cargo, over $4 billion annually, and I think we all agree it is imperative that the necessary cybersecurity resilience practices are utilized at all critical infrastructure including our ports.

That is why I am introducing the Protecting Investments in our Ports with Senator Cornyn to ensure that ports receive digital infrastructure grants from the port infrastructure development program and have cybersecurity procedures in place to protect their digital projects.

So, Mr. Lyttle, in your testimony you mentioned how this attack impacted some of the maritime assets with the Port of Seattle so could you discuss the added complication of this attack being carried out against both aviation and maritime operations and how these systems basically being interconnected may have impacted your response? That would be helpful.

Mr. LYTTLE. Yes. In an environment where it is just an airport environment it is limited maybe to a local area network. With our infrastructure, because we also have the maritime operation, we have a more wider—wide area network or some may consider it a metropolitan area network that is spread across multiple facilities. So that made it more complicated.

One of the good thing is that we have an information technology and information security department that has responsibility for both the maritime institution as well as the aviation institution as well.

So it is more complicated to manage because of the various different locations that falls under that responsibility.

However, as I mentioned earlier, the networks are segmented so some of the services at Maritime Institute was impacted—for example, recreational boating, fishing. Those were impacted but crews were not and the cargo operation was not impacted as well.

Senator PETERS. Very good. Thank you.

Well, I think we all agree that crafting strong and effective cybersecurity requirements is a task that Federal agencies must undertake to ensure safety and security of our critical infrastructure and I certainly appreciate the very detailed discussion that we have had here and my colleagues have had on the need to maximize the amount of cybersecurity teams that they spent on actual security versus compliance, which has been an issue.

We need to streamline those requirements, and I have really good news. It is good to come to a committee hearing with good news.

I introduced a bill with Senator Lankford, the Streamlining Federal Cybersecurity Regulations Act, which is—attempts to try to make compliance with multiple regulatory agencies a whole lot easier and I would certainly welcome my colleagues on this committee to join me in this bill.

And, Mr. Reynolds, thank you. Thank you for your support of this bill in your testimony and I look forward to continuing to work with you on that issue.

Mr. Breyault, something we have seen happens after major cyber incidents is that other bad actors including cyber crime groups use the originating cyber attack to target Americans and commit fraud.

For example, in your testimony you discuss bad actors launching phishing attacks after the recent CrowdStrike incident to defraud victims.

These groups, as you well know, take millions of dollars of hard-earned money from honest folks and a question for you is, what do you recommend for how we could work to prevent and respond to these post-attack fraud incidents? What are your top recommendations?

General REYNOLDS. Thank you, Senator, for the question.

Number one, in the aviation sector consumers do not have any control over when these cybersecurity events happen. All they see is the downstream impact of it—the missed flights, the lost airline miles.

And so I think it is very important that Congress and DOT consider policies that will help consumers recover when incidents that are harming them through no fault of their own happen.

That is why in our testimony we have called for Congress to codify DOT's authority to implement delay compensation regulations, which their rulemaking teed up for this January, as well as requiring that stolen airline miles have the same protection that stolen money has when a scammer gets a hold of my credit or debit card and uses it to run up a bunch of charges.

We think that when those miles are lost that is money that belonged to consumers that they have lost through no fault of their own and that the airlines should be required to compensate them for that.

Senator PETERS. Very good.

Well, thank you. Thank you, gentlemen, again for all your work. Thank you, Madam Chair.

The CHAIR. Again, thank you, Senator Peters. I look forward to working with you on your port security ideas with you and Senator Cornyn. Very, very important.

I know you are just arriving, Senator Markey, but you are a fast study and you might be ready. But if not——

STATEMENT OF HON. EDWARD MARKEY,
U.S. SENATOR FROM MASSACHUSETTS

Senator MARKEY. Ready to go.

The CHAIR. OK. Senator Markey.

Senator MARKEY. Thank you, Madam Chair, and thank you for having this very important hearing.

On July 19, a CrowdStrike IT outage caused mass disruptions across multiple critical sectors of the U.S. economy. While the outage itself was not a cyber attack it laid bare the vulnerabilities of our connected IT systems and put a spotlight on the chaos that can erupt when these systems are not protected.

Mr. Breyault, yes or no. Do you agree that airline consumer protection policies are an important part of an airline's broader cyber strategy?

Mr. BREYAULT. Yes, Senator.

Senator MARKEY. And from my perspective, no matter how much airlines prepare there will still be disruptions and we are going to have to be ready to support travelers, OK, and so we thank you for that.

As we saw with the CrowdStrike outage or the cyber attack on the Port of Seattle disruptions, even if resolved quickly, have serious consequences for travelers. In the case of the CrowdStrike outage thousands of consumers were left stranded and confused about their rights as travelers.

The recent FAA reauthorization act took important steps toward protecting consumers in these scenarios. I am particularly proud that the law contained my provision requiring airlines to provide travelers with an automatic refund in the case of a flight delay or cancelation if the consumer does not accept a rebooking or a voucher.

In many ways, the CrowdStrike incident was a stress test for this important provision. Unfortunately, reports suggested that airlines were failing to comply with this provision, arguing that it had not taken effect.

As I explained in a bipartisan letter with Senator Josh Hawley, that just is not true.

General Reynolds, we just heard that the treatment of consumers during a cyber-related event must be a part of a broader cybersecurity plan. Will your members commit to following the law and providing automatic refunds when required such as during a disruption caused by a cyber attack?

General REYNOLDS. Thank you, Senator.

Yes, we would comply fully with all the laws and regulations.

Senator MARKEY. So that means you will, in fact, provide for the refunds?

General REYNOLDS. If that is what the law provides then—again, I am not an accommodation expert. I would defer to our folks that actually work in this range.

Senator MARKEY. Well, it is absolutely critical that there be compliance. The harm is real. The airlines have to protect against it, and if not and the flight does not take off it is the responsibility of the airline.

You just have to continue to update, update, update, update, update. It is a corporate responsibility to spend the money to protect and when they do not and there is a successful attack it is just because the protections were not built in.

Flight disruptions over the past few years have further made clear that refunds and vouchers are not enough to make consumers whole.

So, Mr. Breyault, I want to walk through a couple of scenarios with you. If a flight cancelation, whether from a cyber attack or maintenance issue, causes a traveler to miss a Taylor Swift concert or an NBA game, does the traveler get reimbursed for the event ticket?

Mr. BREYAULT. No, Senator.

Senator MARKEY. What about the cancelation—what if the cancelation causes a stranded traveler to miss a shift at work, losing crucial income that that family was counting on? Does an airline compensate them for that lost income?

Mr. BREYAULT. No, Senator.

Senator MARKEY. And if a passenger misses their kid's birthday party or school play—well, let us be honest, no amount of money can truly make up for missing those special moments.

But you all get the idea here. This is a loss that these families suffer. So whether a flight delay or cancelations is caused by a cyber attack, thunderstorm, or maintenance issue, the costs for a traveler extend far beyond the flight ticket.

Europeans understand this. That is why Europe requires airlines to provide a cash payment to passengers for significant flight delays and compensation beyond refunding a ticket or reimbursing a passenger's hotel room and airport transportation.

U.S. travelers deserve similar protections and that is why I am so pleased that the Biden-Harris administration plans to issue a proposed rule requiring airlines to provide compensation to consumers when a flight delay or cancelation is the airline's own fault.

Mr. Breyault, do you agree that requiring cash compensation for delayed and canceled flights that are the fault of the airline is an important component of protecting consumers?

Mr. BREYAULT. Yes, Senator.

Senator MARKEY. Thank you. So this type of regulation is long overdue and is the third C in my three Cs of consumer protection: communication, correction and compensation.

When airlines screw up they must communicate passengers' rights and options. They must correct their mistake by providing automatic refunds and now we need to make sure airlines compensate passengers when the flight disruption is within the airline's own control.

So I look forward to working with both the National Consumers League and the airlines on this issue. The leading company EMC was in Massachusetts—is in Massachusetts, and when I asked the CEO why do we keep having these successful cyber attacks he said, in most instances the CEO just did not want to spend the extra money to upgrade.

You just have to keep doing it. It is a cost of doing business, and when they do not do it there is going to be a price and we just cannot have it be passed on to consumers. It is not their fault.

It is the airlines' if they did not do it and they should not have to swallow a $1,000 Taylor Swift ticket, you know, because the airline did not build in the protections.

So we thank you, Madam Chair, and a great hearing. Thank you.

The CHAIR. Thank you, Senator Markey, and thank you for your leadership in the FAA bill and getting those provisions to protect consumers, and, yes, we are hearing more about the theft, particularly today, of the mileage program and the need to protect that.

So but, again, appreciate your leadership and communication on this.

I am just going to ask a couple of just roundup questions and I think we are done with other members here, and then we will adjourn.

But one of the key messages from today is the need for communication and I want to clarify now what is that immediate step on impacting that communication—best practices. We know that there is an ARC process at the FAA on cybersecurity. Much bigger picture. That is going to take a while.

But what now are we doing? So, Mr. Lyttle, who is the lead investigator on this attack? Is it the FBI or——

Mr. LYTTLE. Yes, the FBI is.

The CHAIR. OK. And then what would you—what would the witnesses suggest is the best communication framework right now until the ARC process works to communicate to other airports the best practices and things that should be implemented from this?

I would like to see a list. One of the reasons we gave the NTSB a report requirement—an annual report requirement—because we did not feel like people were emphasizing enough next steps after some of their indications from accident reports what should happen.

And so they have now done that and I thought it was very successful. They came before the Committee and basically said, yes, these near misses are not getting addressed, and then the next day the then Acting Administrator convened and put out a requirement.

So here we are trying to get the same level of response. What would you suggest, Mr. Breyault or General Reynolds, too—what in the near term is that—is that process?

Mr. BREYAULT. So, Senator, from a consumer point of view, clear communication and actionable communication from airlines to consumers is incredibly important. From the time that the breach or the cybersecurity incident will first impact their travel consumers need to be made aware of that.

Consumers often show up at an airport and the CrowdStrike instance, and we heard—we saw report after report that consumers were confused. They did not know what was going on.

They were getting mixed messages from the airlines and other sources about what the status was of their flight and if they were going to have to wait 30 minutes or if the flight was going to get canceled.

So I think it is really important that any cybersecurity response plan have a component in there about communicating with the passengers about how this will impact the flight that they are waiting for at the airport that day or the flight that they are going to leave home early in the morning to catch the next morning.

The CHAIR. Mr. Reynolds, since this is an airport issue but it affects airline capacity what do you think the tool is for right now streamlining best practices and communicating that?

General REYNOLDS. Senator, that is a very important question. The industry relies heavily on standards and in fact it has been founded on standards in many ways and it has driven our safety record to the level it has largely because of standards.

I would start there. It does take time to create the standards. It does take time to actually—you start with the best practice. Then you start moving into the standards. I think the tabletop exercise we all talked about I think that is also a very effective way for us to communicate with one another.

We also participate with the Aviation Information Sharing and Analysis Center to share information back and forth with their members and our members as well.

And I think the other part too I would just referenced is that any opportunity for us to work closely with the Federal Government, either working groups or opportunities for us to share lessons learned, is beneficial for not just the industry but also for the government as well.

The CHAIR. Well, I think—does that exist right now? I am saying I do not—I am not sure that exists, that framework, right now.

General REYNOLDS. We are working with—on the information sharing we are working with TSA, FAA and others to develop and work with them on this very topic, information sharing.

The TSA, in fact, they have an air domain analysis—an intelligence and analysis cell that has been very helpful. They lead in this case. We have meetings with them every day to talk about what is happening in the environment.

There seems to be a really nice set of progress checks with them and the FAA and others to find ways in which we can improve information sharing. But it is—it is in the early stages.

The CHAIR. Yes, I am just—I keep thinking about NARUC and I was looking up trying to figure out the—remember the—what its acronym stands for but it is basically a voluntary utility organization that decades ago did the same practice. Why? Because they were being impacted so much.

And so I think that we have to figure out here how to formalize this now while the ARC rulemaking process at FAA is going through to see what we can get from just communication—a daily communication.

As was said, people want to know, well, what is the next best thing to implement, and I am pretty sure here it is going to be related to hygiene, which is pretty simple and pretty basic, but something that could get emphasized.

And so maybe that is—maybe that is the FAA, you know, putting that notice out or maybe it is also the industry working collaboratively, and so that is what I think. We need both.

In my opinion, we need both because the industry can work very collaboratively, very quickly, and they know the systems they are trying to improve.

One thing, General Reynolds, since you are here in our state there has been a lot of collaboration with the Guard and Reserve because there are so many people who work in IT and are state Guardsmen, and they would like to play a more active role here.

So when you talk about the workforce shortage you are thinking, well, what could they do to just, you know, hammer home this hygiene issue and be part of a response.

I do not know if you have any comments on that.

General REYNOLDS. Absolutely, ma'am. I have business cards I will hand to you and if you have anyone who is interested in joining the airlines we would love to have them.

Phenomenal capability. I am very familiar with the folks up there in your state. Phenomenal capability because they have their day job. They know the—the insights they can bring to the military is phenomenal.

So appreciate you mentioning them. The Guard and Reserves do a phenomenal job in this space.

The CHAIR. Well, I think they know what is their job, to protect us on critical infrastructure. So we have had this discussion with them in Washington—in the state of Washington—on cybersecurity for many years and I know—I think I had Senator Murkowski come to an event on this many years ago when we were looking at vulnerabilities, particularly in schools.

But and they were active and they had been deployed. There was a lot of cooperation between entities. But as this need continues to grow and it is not just going to be in the aviation sector—other sectors—where are we going to get that workforce and how are we going to get these evangelists out there communicating to people.

But I thank everybody here. I think the key takeaway is better protection for consumers on million miler program, better communication to airport infrastructure and airport employees to harden our resources.

This is a growing issue. It is not going to shrink. The best way to do it is communicate what we need to do to harden those resources.

Is that right? Is that the—OK.

Well, I thank all the witnesses. You have—the record will remain open for four weeks until October 16. Any Senators who would like to submit questions do so by October—by that time, and then two weeks from now we will have the record complete.

So thank you so much. I appreciate your willingness to respond to our colleagues.

We are adjourned. Thank you.

[Whereupon, at 11:49 a.m., the hearing was adjourned.]

A P P E N D I X

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARIA CANTWELL TO LANCE LYTTLE

Question 1. In your written testimony, you highlighted the efforts of the team at the Seattle-Tacoma International Airport in contributing to the ultimate resilience of the airport's response to the cyberattack.[1] Specifically, you mentioned successful partnerships with airlines, Federal agencies, and tenants,[2] and how employees demonstrated thorough knowledge of primary, backup, and manual systems.[3] What are some ways the aviation industry can cultivate this resilience ahead of a crisis? What can Congress do to help?

Answer. The best ways for the aviation industry to cultivate resilience is to increasingly engage—both individually and collectively—in emergency preparedness. The processes to become resilient are not necessarily complex, but instead take commitment, time and focus. From conducting tabletop exercises and drills to developing Continuity of Operations (COOP) plans, the more that aviation stakeholders participate in these efforts, the better that we can jointly respond during actual incidents.

One of the best ways to make progress on this front is to work collectively to standardize and disseminate these emergency preparedness best practices throughout the aviation industry. The Port of Seattle and SEA are looking forward to being able to share our own lessons learned to help develop tabletop exercises with specific scenarios informed by our experience, and we know that there are opportunities to learn from others who have gone through similar incidents.

To achieve this best practices sharing, we are engaging with a number of existing forums, such as our industry associations, existing Federal committees, and other annual aviation gatherings. We look forward to partnering with Airports Council International, the American Association of Airport Executives, Airlines For America, and others in this work.

We also welcome Congress to help coordinate these planning and best practices sharing exercises between the industry and the Federal government. There are two specific actions that Congress could consider. First, the Federal Emergency Management Agency already has a National Preparedness Goal that emphasizes public/private partnerships and includes a variety of best practices such as joint exercises and after-action reports; Congress could be very impactful in helping to elevate these foundations, and encourage private sector participation.

Second, it would be very helpful for Congress to examine the current regulatory and reporting structure related to Federal cybersecurity oversight. There are a number of Federal agencies with different jurisdictions, different regulations, and different expertise connected to various aspects of the aviation industry—from the Federal Aviation Administration and the Transportation Security Administration to the Cybersecurity and Infrastructure Security Agency (CISA) and the National Institute of Standards and Technology (NIST). If there can be a more streamlined system for airlines and airports to share information with—and get feedback from—the Federal government, it will benefit everyone. If needed, there are proposed legislation that would make these changes in a formal way. At the very least, Congress could help provide more clarity on the roles of different agencies, and how information flows to one central point of contact.

Of course, one of the most valuable things Congress could do is provide Federal grants to various actors within the aviation industry to allow for greater investments in cybersecurity—from planning and staffing to hardware and software. Many airports do not have a dedicated emergency management professional on staff,

---

[1] *Aviation Cybersecurity Threats,* 118th Cong. (Sept. 18, 2024) (Written Testimony of Mr. Lance Lyttle, Aviation Managing Director, Seattle-Tacoma International Airport), *https://www.commerce.senate.gov/services/files/A254A80D-EB70-4F21-BAD4-5ACF13CA6088* at 7.

[2] *Id.* at 8.

[3] *Id.* at 3.

nor the resources to prepare for the increasingly sophisticated and complex threat actors. This funding would not only have value in terms of the actual dollars invested, but also send a clear signal that cybersecurity as an increasingly core part of the aviation system's operations and resiliency.

Question 2. During this hearing, both you and Brig. Gen. Reynolds emphasized the importance of information sharing, within and between airlines, airports, and governments, to improve cybersecurity defenses.[4]

1) What speciﬁc information is most helpful in helping guard against cyberattacks?

2) What is currently hindering that ﬂow of information?

Answer. There are two broad areas that we would welcome continuing and enhanced information sharing between the aviation industry and the Federal government. First, government agencies should continue to proactively prioritize the dissemination of timely and actionable cyber threat information as soon as reasonably practicable. For example, classified briefings should be provided at the earliest opportunity to highlight new and emerging threats. In particular, it is most helpful that—in the face of increasingly sophisticated threat actors—shared intelligence should be proactive rather than reactive, focused on identifying advanced persistent threats in advance of cyberattacks. Ideally, this information would be as specific as possible, not just who is operating but also detailed, actionable data like firewall logs and other identified activity.

Of note, CISA already has an Automated Indicator Sharing (AIS) service which is designed to support these efforts, but a recent Department of Homeland Security Office of Inspector General report found that use of this system has fallen to its lowest level since 2017, with a 93 percent decline in the sharing of cyber threat indicators from 2020 to 2022. Reviving this service could be a valuable step for Congress and the Federal government to focus on.

Second, airports and airlines welcome Federal feedback on the variety of plans and procedures that we submit to the Federal government, as required by various regulations. Currently, that information sharing is a "one-way street" in that we submit our plans, but we do not get feedback on our submissions nor do we learn best practices from other stakeholders' reporting. If there were a way for Federal agencies to synthesize and re-share key insights from peers, we would all benefit. In fact, these summaries of best practices would be an excellent way to inform future cyber regulations, particularly as TSA continues to evolve its role overseeing airports in this regard.

In terms of what is hindering the flow of information, there is definitely room for increased streamlining about who reports what to which agency, as mentioned above. Cybersecurity regulations should be outcome-focused, risk-based, appropriate, and proportionate to the threat. For airports in particular, it is also important that they are operationally viable and economically sustainable, and that they minimize any duplicative or contradictory guidance. The fewer forms and submissions we are required to submit, the more we can focus on operations. This point is particularly true for smaller airports who do not have the staffing and resources to dedicate to these issues.

For example, we would all benefit from greater clarity about how the NIST Cybersecurity Framework and CISA's Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) notice of proposed rulemaking fully integrates with TSA cybersecurity mandates. These improvements could ensure that the proper information is collected and distributed in the most efficient manner. We would welcome Congress to help ensure this coordination.

Response to Written Questions Submitted by Hon. Raphael Warnock to John Breyault

Question. During an event with mass flight delays and cancellations, including one caused by a cyberattack or disruption, is it important for airlines to immediately and clearly communicate with their customers about the protections to which they are entitled, including any hotel, meal, or transportation vouchers and reimbursements?

Answer. Yes. Unless they commit to doing so via their Customer Service Plan,[2] air carriers are not required under Federal law to provide hotel, meals, or transpor-

---

[4] *Supra* note 5; Aviation Cybersecurity Threats, 118th Cong. (Sept. 18, 2024) (Statement of Mr. Lance Lyttle, Aviation Managing Director, Seattle-Tacoma International Airport), *https://www.commerce.senate.gov/2024/9/aviation-cybersecurity-threats.*

[2] 14 CFR 259.5 Online: *https://www.ecfr.gov/current/title-14/section-259.5*

tation vouchers and reimbursements in the event of a mass delay or cancellation.[3] At a time when passengers may be stranded in an unfamiliar city for an indeterminate amount of time, it is critical that passengers receive clear, actionable information about their rights in a timely manner from their air carrier.

Question. During an event with mass flight delays and cancellations, if an airline fails to immediately and clearly communicate with travelers about the full range of protections to which they are entitled, how might that affect a consumer's decision making?

Answer. In the event of mass flight delays and cancellations, it is crucial that passengers receive clear, actionable, and prompt information about the protections to which they may be entitled. The protections to which a passenger may be entitled can also be affected by the reason for the delay or cancellation and whether the reason was controllable by the air carrier. For example, a mechanical failure on an aircraft is typically considered a controllable reason for a delay or cancellation, while a weather-related delay or cancellation may not be considered controllable. Absent clear communication from their air carrier, passengers could be harmed by, for example, booking a hotel room with their own funds when they could be entitled to a hotel voucher from their air carrier.

Question. Recognizing that cyberattacks and disruptions also have a real-time effect on travelers, and in order to create a more predictable and thriving ecosystem for travelers, should Congress revisit the costs that airlines are required by law to reimburse to consumers during these events?

Answer. Yes, NCL supports requiring air carriers to provide compensation to passengers affected by cyberattacks and disruptions. U.S.-based carriers already provide compensation and care (food, lodging, and ground transportation) when they operate in jurisdictions that mandate these protections, like the European Union and Canada, but these same carriers do not compensate travelers within the U.S. to the same extent, if at all. Should Congress consider legislation to require such compensation, NCL would be happy to be a resource.

Question. What more should Congress do to ensure airlines adhere to the protections authorized in the FAA Reauthorization Act of 2024, especially during mass disruption events?

Answer. To ensure that air carriers adhere to the protections authorized in the FAA Reauthorization Act of 2024, Congress should appropriate funds to fully support the newly-created Office of Aviation Consumer Protection within DOT.[4] In its advice and consent role, the Senate should ensure that the Assistant Secretary the President nominates to lead the office demonstrates a commitment to airline passenger protection and vigorous enforcement of statutory requirements, including those authorized under the Reauthorization Act. Especially during mass disruption events, air carriers should not be allowed to shirk their responsibilities to protect affected passengers.

Question. What further actions, beyond legislation like the FAA Reauthorization Act, can the government take to protect consumers in these scenarios?

Answer. Earlier this year, NCL, along with eight other consumer organizations, urged President Biden and Transportation Secretary Buttigieg to prioritize the implementation of a range of statutorily-required consumer protection rulemakings, including establishing minimum seat size standards, improving the reporting of causes of flight delays, and ensuring that customer service channels are staffed by live agents.[5] Regulations promulgated pursuant to these statutory directives will benefit, both directly and indirectly, passengers who are affected by future mass delays and cancellation. Through its oversight function, Congress should ensure that

---

[3] Department of Transportation. "Fly Rights: A Consumer Guide to Air Travel" ("Each airline has its own policies about what it will do for delayed passengers waiting at the airport; there are no Federal requirements. If you are delayed, ask the airline staff if it will pay for meals or a phone call. Some airlines, often those charging very low fares, do not provide any amenities to stranded passengers. Others may not offer amenities if the delay is caused by bad weather or something else beyond the airline's control.") (August 7, 2024) Online: *https://www.transportation.gov/airconsumer/fly-rights#Delayed-and-Cancelled-Flights*

[4] "FAA Reauthorization Act of 2024, Title V, Subtitle A, Section 501: Establishment of Office of Aviation Consumer Protection." Public Law No. 118–63, 2024. Online: *https://www.congress.gov/bill/118th-congress/house-bill/3935/text*

[5] "Letter from National Consumers League, *et al* to President Joe Biden and Secretary Pete Buttigieg Regarding Implementing FAA Reauthorization Consumer Protection Mandates." (May 28, 2024) Online: *https://nclnet.org/wp-content/uploads/2024/05/Advocates-FAA-reauth-implementation-letter-May-2024-FINAL-AS-SUBMITTED.pdf*

these and other passenger protection rulemakings are conducted on a timely basis and substantively reflect the will of Congress.

Additionally, Congress should explicitly codify DOT's authority to establish critical consumer protection rulemakings, like the Full Fare Advertising Rule (which requires airlines to include all mandatory charges within the advertised price),[6] the Ancillary Fee Transparency Rule (which requires airlines to disclose the cost of baggage, change, and cancellation fees),[7] and the announced rulemaking on delay compensation (which is likely to require airlines to compensate consumers who experience significant delays or cancellations, similar to protections in place in the European Union and Canada).[8] While NCL is confident that the Department already has statutory authority to promulgate these regulations under its ability to prohibit unfair and deceptive practices, several major airlines and Airlines for America have brought a lawsuit seeking to remove the Department's regulatory ability under 49 USC 41712.[9] Should Congress codify DOT's authority in these areas, it would reduce uncertainty regarding air carriers' responsibilities under the law.

APPENDIX A

Crowdstrike and Consumer Protections

On July 19, 2024, cybersecurity company CrowdStrike released flawed software to Falcon Sensor, their hacking and intrusion vulnerability scanner, which disrupted millions of computers across the United States that use the Windows operating system.[10] This software outage led to thousands of flight delays and cancellations on multiple carriers, stranding travelers at airports like Hartsfield-Jackson International Airport in Atlanta.[11] Many travelers were stuck in long lines and on long holds trying to speak with airline customer service representatives and received incomplete or delayed information about the hotel, meal, and alternative travel vouchers or reimbursements to which they were entitled under the law.[12] This meltdown affected individuals traveling on vacation, children separated from their parents, families who missed their chance to see loved ones, and countless others who just wanted to get home.[13] Both airlines and their customers rely on certainty and predictability when they fly and Congress must ensure that the travel ecosystem upholds basic protections and communication guidelines that support travelers and airlines alike.

1. During an event with mass flight delays and cancellations, including one caused by a cyberattack or disruption, is it important for airlines to immediately and clearly communicate with their customers about the protections to which they are entitled, including any hotel, meal, or transportation vouchers and reimbursements?

2. During an event with mass flight delays and cancellations, if an airline fails to immediately and clearly communicate with travelers about the full range of protections to which they are entitled, how might that affect a consumer's decision making?

3. Recognizing that cyberattacks and disruptions also have a real-time effect on travelers, and in order to create a more predictable and thriving ecosystem for travelers, should Congress revisit the costs that airlines are required by law to reimburse to consumers during these events?

---

[6] 14 CFR 399.84. Online: *https://www.ecfr.gov/current/title-14/chapter-II/subchapter-F/part-399/subpart-G/section-399.84*

[7] "Enhancing Transparency of Airline Ancillary Service Fees." (April 30, 2024) Online: *https://www.federalregister.gov/documents/2024/04/30/2024-08609/enhancing-transparency-of-airline-ancillary-service-fees*

[8] Department of Transportation. "DOT to Propose Requirements for Airlines to Cover Expenses and Compensate Stranded Passengers." (May 8, 2023). Online: *https://www.transportation.gov/briefing-room/dot-propose-requirements-airlines-cover-expenses-and-compensate-stranded-passengers*

[9] Associated Press. "US airlines are suing the Biden administration over a new rule to make certain fees easier to spot." (May 13, 2024) Online: *https://apnews.com/article/airlines-sue-biden-administration-junk-fees-346ad8ad06335587ba8a67240c5cda32*

[10] *External Technical Root Cause Analysis—Channel File 291,* CrowdStrike (Aug. 6, 2024), *https://www.crowdstrike.com/wp-content/uploads/2024/08/Channel-File-291-Incident-Root-Cause-Analysis-08.06.2024.pdf.*

[11] Christine Chung, *Stranded in the CrowdStrike Meltdown: 'No Hotel, No Food, No Assistance,'* New York Times (Sept. 13, 2024), *https://www.nytimes.com/2024/09/13/travel/crowdstrike-outage-delta-airlines.html.*

[12] *Id.*

[13] *Id.*

Consumer Protection

The Federal Aviation Administration (FAA) Reauthorization Act of 2024, P.L. 118–63, guarantees airline passengers the right to a full refund in the case of a cancelled or significantly delayed or changed flight if that passenger chose not to fly on the delayed or changed flight or accept rebooking to an alternative flight and did not otherwise accept any voucher or other form of compensation.[14] Yet, after the flight cancelations stemming from the CrowdStrike outage in July, the Department of Transportation was forced to open an investigation into some airlines' treatment of passengers' refunds.[15]

1. What more should Congress do to ensure airlines adhere to the protections authorized in the FAA Reauthorization Act of 2024, especially during mass disruption events?

2. What further actions, beyond legislation like the FAA Reauthorization Act, can the government take to protect consumers in these scenarios?

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. RAPHAEL WARNOCK TO MARTY REYNOLDS

Local Government Airport Costs

Across the country, airports deliver economic benefits for communities through increased employment, visitor spending, business investment, and more.[1] According to a 2020 report from the Georgia Department of Transportation, Georgia's airports support over 450,000 statewide jobs and nearly $73.7 billion in economic activity.[2] A large portion of this economic activity is generated by Hartsfield-Jackson Atlanta International Airport, the world's busiest airport.[3] For many communities, the economic development driven by the local airport helps support the transportation, public safety, and education costs associated with hosting that airport.[4] Unfortunately, Clayton County, Georgia, home of Hartsfield-Jackson Atlanta International Airport, does not own or operate the airport in its community.[5] Because of this, Clayton County bears the many costs associated with hosting a major commercial airport, but does not receive the full benefits enjoyed by other jurisdictions who own and operate the airports located in their communities, resulting in limited funding to support the airline and airport employees who live in Clayton County and rely on its services.[6] That is why I authored a provision, which was unanimously supported by the Senate Committee on Commerce, Science, and Transportation, that would have allowed Clayton County to access funding afforded to every other airport host community.[7] Unfortunately, this provision was not included in the Federal Aviation Administration Reauthorization Act of 2024, P.L. 118–63.

Question 1. Is it the understanding of Airlines for America that local governments bear costs associated with hosting the Nation's airport and airlines, including costs associated with transportation, security, and education for airport and airline employees?

Answer. A4A is not aware of, and does not maintain, information on specific municipalities across the country. However, A4A does agree that airports are significant economic engines for the local communities they serve. Every U.S. airline job helps support 9 additional jobs. The operating and capital costs of those commercial airports are paid for by revenues collected from airlines, their passengers and other

---

[14] FAA Reauthorization Act of 2024, Pub. L. No. 118–63 § 503(a)(a); 49 U.S.C. § 42305.

[15] Kyle Potter, *How Delta (Repeatedly) Bungled its Worst Meltdown Ever,* Thrifty Traveler (July 26, 2024), *https://thriftytraveler.com/news/airlines/delta-meltdown-recap/*; *https://www.cnn.com/2024/08/07/business/delta-passengers-sue-crowdstrike-meltdown/index.html;* Tara Suter, *Feds launch investigation into Delta after flight fiasco,* The Hill (July 23, 2024), *https://thehill.com/policy/transportation/4787799-dot-investigation-delta-flight-cancellations/*

[1] *Taking America Beyond the Horizon, The Economic Impact of U.S. Commercial Airports in 2017,* Airports Council International—North America (Nov. 2018), *https://airportscouncil.org/intelligence/economic-impact-study/*.

[2] *Statewide Airport Economic Impact Study,* Georgia Department of Transportation (Oct. 2020), *https://www.dot.ga.gov/GDOT/Pages/AirportEIS.aspx.*

[3] *Id.*

[4] Joe Henke, *Eliminating jet fuel tax could cost Clayton County schools,* 11Alive (Feb. 10, 2018), *https://www.11alive.com/article/news/local/eliminating-jet-fuel-tax-could-cost-clayton-county-schools/85-517207329.*

[5] Leon Stafford, *Clayton Schools eyeing Hartsfield-Jackson as tax revenue source,* Atlanta Journal-Constitution (Nov. 20, 2019), *https://www.ajc.com/news/local/clayton-schools-eyeing-hartsfield-jackson-tax-revenue-source/auKU1h5FV8O2zgKMVRe2UM/*.

[6] *Id*

[7] FAA Reauthorization Act of 2024, S. 1939, 118th Cong. § 624 (2023).

users of the airport. The rules that govern how those airport revenues can be used is subject to a longstanding and successful Federal Aviation Administration (FAA) revenue use policy.

Question 2. Is Airlines for America aware of any other local government in the United States that has a major airport located in its jurisdiction but neither owns nor operates that airport?

Answer. A4A is not aware of, and does not maintain, information on specific municipalities across the country. We would recommend your office contact the FAA for any additional information.

Aviation Fuel Sales Tax Revenue

49 U.S.C. 47133(a) provides that local taxes on aviation fuel must be spent on the "capital or operating costs" of specific eligible entities: (1) an "airport," (2) "local airport system," or (3) "any other local facility . . . that is directly and substantially related to the air transportation of passengers or property."[8]

Question 1. If a local government does not own or operate any of the entities described under 49 U.S.C 47133(a)(1)-(3), what is Airlines for America's position on for what purposes could such a local government expend local sales tax revenues collected on the sale of aviation fuel?

Answer. A long-standing principle of that aviation policy supported by A4A is that fuel-related taxes must be used to benefit the users of the respective transportation system. In 1987, Congress explicitly recognized this principle for aviation fuel by enacting the Airport and Airway Safety and Capacity Expansion Act of 1987 (Act) that broadly and directly prohibited taxes on aviation fuels unless the proceeds were used for airport capital or operating costs, or state aviation programs (in the case of state aviation fuel taxes).[9]

Since its enactment, the FAA has consistently interpreted the Act to apply to any state or local tax on aviation fuel, whether the tax specifically targeted aviation fuel or was a general sales tax on products that included aviation fuel.[10] Additionally, the FAA has interpreted the Act to make no distinction between taxes imposed by a local government or state agency.

The only exception to the Act applies to fuel-related taxes that were levied prior to 1987, which fall under a grandfather clause. However, if a tax is repealed and later reinstated or increased at any time, the tax (or the amount it is increased by) is no longer grandfathered.

This use of fuel-related taxes is vital to airport operations because states and airports that receive funding from the FAA for airport improvement projects are subject to the Federal rules and regulations implementing these statutes. Compliance with these statutes keeps airports eligible for the FAA Airport Improvement Program (AIP).

In 2014, the FAA finalized a policy statement reiterating its interpretation that the Act applies to taxes on fuel, including general sales taxes, whether imposed by a state or local jurisdiction. In addition, the FAA announced that the Federal government would allow a three-year transition period for taxing authorities to comply with Federal law; that period expired over five years ago on December 8, 2017.[11]

In that policy statement, the FAA reiterated that Congress clearly intended the Act to apply to taxes collected from the sale of aviation fuel and other products. The FAA further reiterated that requiring aviation use of local government proceeds—but not state proceeds—from taxes on aviation fuel would substantially undermine the purpose of the Act and be inconsistent with congressional intent. The FAA then cited its five previous opinions regarding state and local taxes on aviation fuel to confirm that this policy statement was in fact a reaffirmation of existing policy and not a policy change.

Pursuant to Federal law, aviation fuel tax revenues must be used for aviation purposes. For additional information, the FAA's website and docket on this topic and be found at: *https://www.faa.gov/airports/airport_compliance/aviation_fuel_tax*

Clayton County, Georgia Aviation Fuel Sales Tax Revenue

The Atlanta Hartsfield-Jackson Airport is located within the boundaries of Clayton County, Georgia, yet the government of Clayton County neither owns nor operates the Atlanta Hartsfield-Jackson Airport or any other eligible entity under 49

[8] 49 U.S.C. § 47133.
[9] 49 U.S.C. §§ 47107(b) and 47133.
[10] The FAA interpreted this legislation in 1990, 1992, 2000, 2009, 2010, and 2014.
[11] Policy and Procedures Concerning the Use of Airport Revenue; Proceeds From Taxes on Aviation Fuel, 79 Fed. Reg. 66282 (Nov. 7, 2014).

U.S.C. 417133(a).[12] Because there exist no eligible uses for revenues obtained on a local sales tax of aviation fuel, Clayton County has ceased collecting sales tax revenues from sales of aviation fuel within its jurisdiction.[13]

Question 1. Do your member airlines routinely purchase aviation fuel?

Answer. Yes.

Question 2. Do your member airlines routinely pay local sales tax on their purchase of aviation fuel?

Answer. Yes. The use of those revenue is subject to the FAA revenue use policy.

Question 3. Would suspending local sales taxes on the purchase of aviation fuel financially benefit your member airlines?

Answer. Local sales taxes on aviation fuel are categorized as expenses to airlines. Measures that reduce expenses benefit any company.

Question 4. Assume that County A collects sales tax on aviation fuel while County B does not. All else equal, would your member airlines benefit financially if they purchased aviation fuel in County B rather than County A?

Answer. It is not possible to answer hypothetical questions without knowing the full context. In general, any measure that reduces expenses is beneficial to any company. That said, any hypothetical revenues collected would be subject to the FAA revenue use policy.

As discussed above, Clayton County does not own or operate Hartsfield-Jackson Atlanta International Airport, although the airport is physically located within Clayton County.

Question 5. Do employees of your member airlines routinely live near their base airport, including in the surrounding county?

Answer. A4A is not aware of, and does not maintain, information on specific municipalities across the country or employee housing location and circumstances.

Question 6. If employees of your member airlines live in the surrounding county near their base airport, and the county operates a public school system, is it Airlines for America's understanding that the county typically expends resources on educating the children of your member airlines' employees?

Answer. A4A is not aware of, and does not maintain, information on specific municipalities across the country or employee housing location and circumstances.

Question 7. Do employees of your member airlines often rely on transportation systems surrounding the airport, including roads, bridges, highways, and transit?

Answer. A4A is not aware of, and does not maintain, information on specific municipalities across the country or employee housing location and circumstances.

Question 8. Do employees of your member airlines ever experience healthcare emergencies while working at an airport, requiring a response from county employees such as ambulance drivers or 911 operators?

Answer. A4A is not aware of, and does not maintain, information on specific municipalities across the country or employee housing location and circumstances.

Question 9. Does Airlines for America agree that local governments typically expend financial resources on services like public schools, transportation systems, and emergency response?

Answer. Yes.

Question 10. Does Airlines for America agree that local governments typically collect sales tax revenues to defray costs of services like public schools, transportation systems, and emergency response?

Answer. Local government tax collections and expenditures are not our area of expertise. A4A does not maintain information on specific municipalities across the country.

Question 11. Does Airlines for America support any Federal law or policy that prevents a local government from collecting sales tax on particular goods, such as aviation fuel, even if the decrease in revenue would harm the local government and impede its ability to provide essential services?

Answer. We strongly support the FAA's longstanding revenue use policy.

Question 12. When Federal law or policy prevents a local government from collecting sales tax on particular goods, such as aviation fuel, does the decrease in tax revenue typically help or hurt the local government?

---

[12] *ATL Fact Sheet,* Hartsfield-Jackson Atlanta International Airport, *https://www.atl.com/about-atl/atl-factsheet.*

[13] *Sales Tax Rates—Jet Fuel,* Georgia Department of Revenue, *https://dor.georgia.gov/sales-tax-rates-jet-fuel.*

Answer. We defer to local governments to determine the best way to manage their budget needs in accordance with Federal law.

Question 13. When Federal law or policy prevents a local government from collecting sales tax on particular goods, such as aviation fuel, does the decrease in tax revenue typically mean the local government can offer more or less services?

Answer. We defer to local governments to determine the best way to manage their budget needs in accordance with Federal law.

Question 14. When Federal law or policy prevents a local government from collecting sales tax on particular goods, such as aviation fuel, does the decrease in tax revenue typically mean the local government has more or less to spend on supporting public schools, transportation, or emergency response?

Answer. We defer to local governments to determine the best way to manage their budget needs in accordance with Federal law.

Question 15. Other than Clayton County, Georgia, is Airlines for America aware of any other jurisdiction in the United States that is home to a major airport that is precluded from collecting sales taxes on aviation fuel under 49 U.S.C. 47133? If so, please list them.

Answer. A4A does not maintain that type of information. We would recommend speaking with the FAA. Additionally, a FAA website that provides information on every state and locality on this issue can be found at: *https://www.faa.gov/airports/airport_compliance/aviation_fuel_tax*

Federal Reporting Requirements for Cybersecurity Incidents

According to the Department of Homeland Security, as of September 2023, there are 45 active Federal cyber incident reporting requirements.[14] Airlines specifically are subject to the reporting frameworks of 10 different Federal departments or agencies.[15] This proliferation of reporting requirements may make compliance more difficult for the airline industry.

Question 1. How consistently does the airline industry comply with Federal reporting requirements currently? Are there some compliance requirements that are disproportionately burdensome?

Answer. A4A-member airlines comply with all laws and regulations including those relating to cybersecurity. The most burdensome compliance challenge is the lack of harmonization across the Federal government for reporting cyber incidents. Airlines are currently subject to 10 different Federal departments and agencies with existing or proposed, mandatory and voluntary incident reporting frameworks. It is important to note that the requirements of these 10 Federal agencies differ on definitions, thresholds, processes, timelines, data protections, compliance regimes and content requirements.

Question 2. Having interacted with so many agencies, are there practices that stood out to you as helpful that some agencies do that others do not? If so, which ones and why?

Answer. A4A believes the most effective cybersecurity programs are risk-based, threat-informed and constantly evolving to stay ahead of a dynamic threat landscape. Our member's cybersecurity programs and investments are based on these foundational principles.

A4A does not have a specific agency model to emphasize, however, along with the cyber incident reporting harmonization outlined above, it is paramount that Federal agencies also improve and strengthen information sharing with other regulators, the intelligence community, and private stakeholders to improve the speed and relevance of shared information.

Although Federal agencies have made strides to improve information sharing such as multi-agency threat bulletins, the information airlines receive from Federal agencies is often not timely or consistent. One promising effort is being led by the Transportation Security Administration (TSA) which is currently developing an interagency information sharing working group that includes the FAA, Cybersecurity and Infrastructure Security Agency (CISA) and the Department of Defense (DoD).

---

[14] *Harmonization of Cyber Incident Reporting to the Federal Government,* Department of Homeland Security, Office of Strategy, Policy, and Plans (Sept. 19, 2023), *https://www.dhs.gov/sites/default/files/2023-09/Harmonization%20of%20Cyber%20Incident%20Reporting%20to%20the%20Federal%20Government.pdf* at 4.

[15] *Aviation Cybersecurity Threats,* 118th Cong. (Sept. 18, 2024) (Written Testimony of Mr. Marty Reynolds, Brigadier General, USAF (Retired), Managing Director for Cybersecurity, Airlines for America), *https://www.commerce.senate.gov/services/files/42455719-FD6F-42EC-853B-1F4FA521E867* at 2.

Workforce Development

The cybersecurity industry has a global shortage of workers.[16] This shortage also affects the aviation industry, as you acknowledged during this hearing.[17]

Question 1. What can Congress do to help fill this gap?

Answer. A4A appreciates Senator Warnock's work and focus on building a diverse aviation workforce. Attracting and retaining cybersecurity professionals is critical to the aviation sector's success. Demand for cybersecurity professionals is currently outpacing supply which is a trend projected to stay in place for years. To address the cybersecurity talent management shortage, we recommend Congress consider several potential actions:

- Support grants and initiatives that make it easier to obtain cybersecurity certification, education and training; and
- Collaborate on implementing components of the July 2023, Office of the National Cyber Director's (ONCD), National Cyber Workforce and Education Strategy. This report offers guiding imperatives and recommendations to attract and retain cybersecurity professionals.

○

[16] Michelle Meineke, *The cybersecurity industry has an urgent talent shortage. Here's how to plug the gap,* Centre for Cybersecurity, World Economic Forum (Apr. 28, 2024), *https://www.weforum.org/agenda/2024/04/cybersecurity-industry-talent-shortage-new-report/; Cybersecurity Workforce Demand,* NICE, National Institute of Standards and Technology (June 2023), *https://www.nist.gov/system/files/documents/2023/06/05/NICE%20FactSheet_Workforce%20Demand_Final_20211202.pdf; Dexter Tilo, Cybersecurity industry short nearly 4 million professionals,* HRD America (May 14, 2024), *https://www.hcamag.com/us/news/general/cybersecurity-industry-short-nearly-4-million-professionals/489138.*

[17] *Aviation Cybersecurity Threats,* 118th Cong. (Sept. 18, 2024) (Statement of Mr. Marty Reynolds, Brigadier General, USAF (Retired), Managing Director for Cybersecurity, Airlines for America), *https://www.commerce.senate.gov/2024/9/aviation-cybersecurity-threats.*