

IMPROVING SECURITY AT AMERICA'S AIRPORTS: STAKEHOLDER PERSPECTIVES

HEARING

BEFORE THE

SUBCOMMITTEE ON SECURITY

OF THE

COMMITTEE ON COMMERCE,
SCIENCE, AND TRANSPORTATION
UNITED STATES SENATE

ONE HUNDRED SIXTEENTH CONGRESS

FIRST SESSION

OCTOBER 17, 2019

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



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

U.S. GOVERNMENT PUBLISHING OFFICE

WASHINGTON : 2023

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED SIXTEENTH CONGRESS

FIRST SESSION

ROGER WICKER, Mississippi, *Chairman*

JOHN THUNE, South Dakota	MARIA CANTWELL, Washington, <i>Ranking</i>
ROY BLUNT, Missouri	AMY KLOBUCHAR, Minnesota
TED CRUZ, Texas	RICHARD BLUMENTHAL, Connecticut
DEB FISCHER, Nebraska	BRIAN SCHATZ, Hawaii
JERRY MORAN, Kansas	EDWARD MARKEY, Massachusetts
DAN SULLIVAN, Alaska	TOM UDALL, New Mexico
CORY GARDNER, Colorado	GARY PETERS, Michigan
MARSHA BLACKBURN, Tennessee	TAMMY BALDWIN, Wisconsin
SHELLEY MOORE CAPITO, West Virginia	TAMMY DUCKWORTH, Illinois
MIKE LEE, Utah	JON TESTER, Montana
RON JOHNSON, Wisconsin	KYRSTEN SINEMA, Arizona
TODD YOUNG, Indiana	JACKY ROSEN, Nevada
RICK SCOTT, Florida	

JOHN KEAST, *Staff Director*

CRYSTAL TULLY, *Deputy Staff Director*

STEVEN WALL, *General Counsel*

KIM LIPSKY, *Democratic Staff Director*

CHRIS DAY, *Democratic Deputy Staff Director*

RENAE BLACK, *Senior Counsel*

SUBCOMMITTEE ON SECURITY

DAN SULLIVAN, Alaska, <i>Chairman</i>	EDWARD MARKEY, Massachusetts, <i>Ranking</i>
ROY BLUNT, Missouri	AMY KLOBUCHAR, Minnesota
TED CRUZ, Texas,	RICHARD BLUMENTHAL, <i>Connecticut</i>
DEB FISCHER, Nebraska	BRIAN SCHATZ, Hawaii
MARSHA BLACKBURN, Tennessee	TOM UDALL, New Mexico
MIKE LEE, Utah	TAMMY DUCKWORTH, Illinois
RON JOHNSON, Wisconsin	KYRSTEN SINEMA, Arizona
TODD YOUNG, Indiana	JACKY ROSEN, Nevada
RICK SCOTT, Florida	

CONTENTS

Hearing held on October 17, 2019	Page 1
Statement of Senator Sullivan	1
Statement of Senator Markey	3
Statement of Senator Gardner	4
Statement of Senator Lee	33
Statement of Senator Blumenthal	40

WITNESSES

Tori Emerson Barnes, Executive Vice President, Public Affairs and Policy, U.S. Travel Association	5
Prepared statement	7
Chris McLaughlin, Chief Operations Officer, Denver International Airport	12
Prepared statement	13
Lauren Beyer, Vice President of Security and Facilitation, Airlines for Amer- ica	15
Prepared statement	17
Ken Cornick, Co-Founder and President, CLEAR	20
Prepared statement	22
Sara Nelson, International President, Association of Flight Attendants-CWA, AFL-CIO	24
Prepared statement	25

APPENDIX

Letter dated October 16, 2019 to Hon. Dan Sullivan and Hon. Edward J. Markey from Marc Rotenberg, EPIC President; Caitriona Fitzgerald, EPIC Policy Director; and Jeramie Scott, EPIC Senior Counsel	45
American Federation of Government Employees, AFL-CIO, prepared state- ment	47
Response to written question submitted by Hon. Todd Young to: Tori Emerson Barnes	49
Response to written questions submitted by Hon. Dan Sullivan to: Ken Cornick	50
Response to written questions submitted by Hon. Amy Klobuchar to: Chris McLaughlin	50
Lauren Beyer	51

IMPROVING SECURITY AT AMERICA'S AIRPORTS: STAKEHOLDER PERSPECTIVES

THURSDAY, OCTOBER 17, 2019

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

The Subcommittee met, pursuant to notice, at 10:35 a.m. in room SD-562, Dirksen Senate Office Building, Hon. Dan Sullivan, Chairman of the Subcommittee, presiding.

Present: Senators Sullivan, Blunt, Lee, Markey, Cantwell, Blumenthal, Sinema, and Rosen.

Also present: Senator Gardner.

OPENING STATEMENT OF HON. DAN SULLIVAN, U.S. SENATOR FROM ALASKA

Senator SULLIVAN. Good morning. This hearing on the Security Subcommittee of the Commerce Committee will now come to order.

I am pleased to welcome our distinguished panel of witnesses today. And I apologize for the late start. A couple of us were in hearings on other committees on some topics of the day that kept us a little bit long. But I want to thank them to bring their unique perspectives—our witnesses on airport security.

While the Transportation Security Administration is the principal Federal agency tasked with keeping our transportation system secure, we know that security is a team effort among the private sector and among different Federal agencies.

This hearing will focus on the perspectives of many stakeholders, airports, airlines, employees, technology providers, and the travel industry, on the state of aviation security and where this committee should focus its attention to address the most demanding needs and vulnerabilities in this arena.

The importance of aviation security obviously cannot be overstated. The terror attacks of September 11th showed us how our transportation systems can be used as weapons against our own citizens if not properly guarded.

Following these attacks, we rose to the challenge to secure our airports against future acts of terrorism, but of course, we need to remain vigilant.

One of the most notable actions toward this goal was the creation by the Congress of the Transportation Security Administration. Since its inception at the end of 2001, the TSA has grown and adapted to meet the ever-changing threats across our transportation systems. Like a lot of Senators, I spend a lot of time trav-

eling and in airports almost every weekend, and I always thank our TSA employees, especially in Alaska for the important work that they are doing up in my State.

Nowhere is the adaptability of aviation and the threats more important than in aviation security. U.S. airports accommodate over 950 million domestic and international aviation passengers each year. That means each day the security systems at our airports must be able to screen nearly 3 million passengers, 1.5 million checked bags, and million carry-on bags every day. And this demand on the system continues to grow.

Last month, Acting Deputy Administrator Patricia Cogswell testified before our Full Committee that, quote, the last 12 months represents the highest volume of air travelers in TSA's history with the busiest summer travel season ever and estimates of anticipated annual growth of 4.5 percent per passenger travel over the next 20 years.

Congress has taken action to be ready for this growth most recently by passing the TSA Modernization Act as part of the FAA reauthorization last year. Notably, this legislation marks the first time since its creation that TSA has been reauthorized. In the TSA Modernization Act, we directed the TSA to make significant changes to propel innovation, expand field operations and testing of advanced screening technologies, increase use of canine resources, and enhance public area security.

Now that a full year has passed since this Act was signed into law, we need to ensure that these measures are being implemented in a timely fashion so that we can stay ahead of evolving threats instead of being forced to respond to them. That is the overall purpose of this oversight hearing today.

The application of new security methods and technologies must take into account their effect on commerce. Commercial aviation is a \$446 billion industry that supports over 10 million jobs. We must be able to look for and strike the right balance to implement security that is strong and protects our citizens and critical infrastructure while also being fluid enough to enable the uninhibited flow of legitimate passenger, baggage, and air cargo in commerce. Balancing this risk-based approach is not easy, but it is critical to sustaining a secure environment that enables our industry and the security of our citizens to continue.

The aviation industry needs to continue collaborative efforts and information sharing to address security threats to their businesses and customers. And that is why it is so important for us to hear from many of them on today's panel. The unique perspectives of our witnesses in this hearing are invaluable in terms of identifying how well the TSA is working with their stakeholders to share security-related information, plan the development of new security technology, and respond to the varying needs of individual airports, airlines, and trusted partners across the industry, all with the goal of making sure our citizens are safe.

With that, I want to thank our witnesses for being here today.

And I now recognize Ranking Member Markey for any opening statement.

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

Senator MARKEY. Thank you, Mr. Chairman, very much, and thank you for having this important hearing on aviation security.

Thanks to all the witnesses for being here today. This panel offers us a range of perspectives on what more we need to do to secure our skies.

Twenty years ago, aviation security was handled by private companies employed by the airlines themselves. This system created dangerous vulnerabilities, vulnerabilities that were exposed and exploited on September 11, 2001. Determined to prevent future attacks, Congress created the TSA to Federalize aviation security and ensure that one agency was in charge.

In the years since, Congress has continued to improve TSA policies while debating how to best balance security with civil liberties and enhance the passenger experience. When it comes to security, I believe that we have to continue to heed the call of the 9/11 Commission which described, quote, failures of imagination as a primary reason why those attacks were not thwarted. We must do more than simply prepare our defenses for the kinds of attacks we experienced 18 years ago. We must anticipate the loopholes that terrorists could exploit today and into the future.

That is why when Congress passed a law implementing the recommendations of the 9/11 Commission, I secured a provision that required 100 percent screening of air cargo for passenger aircraft. Nearly 40 percent of all cargo that is carried in America is actually on passenger planes, and it is not owned by the passengers on that plane. This air cargo sits directly under the feet of passengers, and it was not subject to any screening prior to my law.

And when we passed the TSA Modernization Act of 2018, I authored language that directed the TSA to carry out a pilot program testing more advanced screening technologies for carry-on luggage. I will keep fighting to make sure our technology keeps pace with the threats we face.

And I am proud of other progress that we have made too, including common sense reforms that I fought for like banning knives on airplanes, which I worked with Ms. Nelson to put on the books as a law, and ensuring that small airports are just as secure as our larger ones.

At the same time, I have long believed that we need to make sure that our safety does not come at the expense of our civil liberties. When the TSA's Quiet Skies program was exposed, I demanded answers about why air marshals were collecting information about American travelers who were not suspected of any crimes and were not on any terrorist watch list. I am pleased that the TSA has since heeded my call to rein in this privacy-violating surveillance program.

And also, as facial recognition technology has become increasingly integrated into the American travel experience, I have raised significant concerns about the absence of rules of the road for how this biometric technology is used. Travelers deserve the right to say no to sharing their biometric information. TSA must be required to secure that biometric data it and its partners collect, and TSA should be required to prevent any racial bias in its use of this tech-

nology. These safeguards cannot be optional. The flying public deserves enforceable rules that are specific to the unique threats that facial recognition technology poses to American privacy.

And moving forward, there are plenty of other issues that we have to look at in order to secure our airports. One major issue is the ongoing diversion of revenue from the 9/11 security fee that is collected. Congress mandated this fee on airline tickets in order to help finance the cost of protecting our nation's aviation system. In 2013, however, Congress began diverting one-third of the revenue generated by the 9/11 security fee to deficit reduction. That diversion of revenue is unacceptable. TSA needs that revenue to secure our airports and our skies. We should end this harmful policy immediately, and I have introduced legislation with Senator Blumenthal in order to ensure that we accomplish that goal.

And finally, another top area of concern is the danger of insider threats. It is critical that we remain vigilant and ensure that terrorists do not gain access to the internal workings of our aviation system. Protecting programs designed to mitigate this risk must be a top priority. And I hope that we can talk today about the Known Crew Member program which counters inside threats by allowing the TSA to verify the identities of airline employees.

I thank you, Mr. Chairman. A very important hearing especially as we are looking at stories of upwards of 11,000 ISIS fighters who could be back out in business again and creating an area that could be used to begin, once again, to plan attacks against the United States. This is a perfect hearing to begin to talk about the protections we need to have in place.

Senator SULLIVAN. Thank you, Senator Markey.

And I do want to welcome all of our witnesses here today: Ms. Tori Barnes, who is the Executive Vice President of Public Affairs and Policy for the U.S. Travel Association; Ms. Lauren Beyer, the Vice President of Security and Facilitation, Airlines for America; Mr. Ken Cornick, who is the Co-founder and President of CLEAR; Ms. Sara Nelson, who is the International President, Association of Flight Attendants; and Mr. Chris McLaughlin, Chief Operating Officer of the Denver International Airport.

And here to introduce Chris in a little more detail is his outstanding U.S. Senator, Cory Gardner.

Senator Gardner.

**STATEMENT OF HON. CORY GARDNER,
U.S. SENATOR FROM COLORADO**

Senator GARDNER. Thank you, Mr. Chairman. Thank you for allowing me to join the Subcommittee. I am not a Member of the Subcommittee, so it is a privilege to be here to introduce Mr. McLaughlin. Thank you to all the members of the Committee for allowing this opportunity.

I am pleased to be here this morning obviously to welcome Chris McLaughlin, who currently serves as the Chief Operating Officer for Denver International Airport, a role in which he oversees the airport's largest business component.

One of the busiest airports in the nation, Denver International Airport has been forward thinking in its efforts to bolster security while maintaining an excellent experience for traveling Coloradans

and millions of visitors. I have been proud to work with the airport to support their efforts at the Federal level.

Mr. McLaughlin has an impressive range of experience that I think will provide a very unique perspective for today's discussion surrounding airport security. He served several years at the Transportation Security Administration, as well as worked at Air Wisconsin Airlines, Frontier Airlines, our hometown airline, and CLEAR.

Welcome, Mr. McLaughlin. Thank you very much for being here today. Thank you for representing Denver International Airport and the organization. I look forward to hearing your testimony today.

Thank you.

Senator SULLIVAN. Thank you, Senator Gardner.

Each of our witnesses will have 5 minutes to deliver an oral argument, and a longer written statement will be included in the record if you so desire. So why don't we begin with Ms. Barnes?

**STATEMENT OF TORI EMERSON BARNES,
EXECUTIVE VICE PRESIDENT, PUBLIC AFFAIRS
AND POLICY, U.S. TRAVEL ASSOCIATION**

Ms. BARNES. Chairman Sullivan, Ranking Member Markey, members of the Subcommittee, good morning.

I am Tori Barnes, Executive Vice President of Public Affairs and Policy for the U.S. Travel Association.

First, I would like to thank the Committee for passing the Brand USA Extension Act, a bill that will reauthorize the United States' only travel promotion program, which is absolutely vital to growing the U.S. economy and reducing the trade deficit.

And thank you for inviting the broader travel industry to participate in this very important hearing today.

U.S. Travel is the only association that represents all sectors of the travel industry: hotels, airports, state and local tourism offices, car rental companies, theme parks and attractions, and many others. U.S. Travel's mission to increase travel to and within the United States is always conditioned on maintaining the strongest and highest standards of security.

In 2018, domestic travelers spent \$933 billion in the United States, which directly supported 7.7 million American jobs. Travel is vital to the American economy and workforce, and some of the best programs we have to facilitate travel are also ones that strengthen security the most.

And that is why I am here today, to discuss ways that we can improve security and efficiency ahead of the October 1, 2020 deadline for REAL ID enforcement.

The REAL ID Act was passed in 2005, and its full implementation has been put off by a series of extensions intended to give states time to bring their IDs into compliance. Now the Department of Homeland Security has said that the era of REAL ID delays is over, and every American will need a REAL ID license or acceptable alternative such as a U.S. passport to fly next October. But Americans are simply not REAL ID ready.

A U.S. Travel study found that an estimated 182 million Americans are unlikely to have a REAL ID, and 50 percent of Americans

are unaware of the October 1, 2020 deadline altogether. In fact, if REAL ID standards were enforced today, 99 million Americans would not have an acceptable alternative ID, and almost 80,000 travelers could be denied boarding on the first day. If that trend were to continue, over half of a million travelers could be turned away in the first week, costing nearly \$300 million in lost spending.

U.S. Travel has been working with our industry partners to share a consistent message to educate and encourage Americans to get a REAL ID. But we cannot solve this by simply pushing people to the DMV, especially when two states are not yet issuing REAL IDs and are not expected to until next summer.

REAL ID represented the most secure form of identification when it was conceived in 2005, but technology has advanced greatly in the past 14 years. And we have a real opportunity to bring security into the future rather than just working to meet the requirements of the past.

U.S. Travel has outlined four policy proposals to modernize security and avoid chaos at our airports next October.

First, turning travelers away at the checkpoint is just not an option. Congress should immediately direct TSA to work with the private sector to develop procedures for clearing travelers that do not have a REAL ID or acceptable form of identification.

Second, Congress should direct DHS to utilize the existing security and identification features of trusted traveler programs by designating CLEAR and TSA PreCheck enrollment applicants as alternatives to REAL ID. This process should be put in place as soon as possible but no later than October 1, 2020.

Third, Congress should act immediately to modernize the REAL ID Act to allow for mobile devices and web-based REAL ID applications and to permit TSA to accept mobile or digital REAL ID-compliant driver's licenses.

Fourth, DHS should accelerate the implementation of biometric identity verification technology at TSA checkpoints. This is simply a way to provide faster, more secure screening, using information that trusted travelers and passport holders have already provided to DHS. Importantly, we are in support of strong, clear standards for accuracy, privacy, and performance mandated by DHS and Congress that drive biometric technology forward.

Let me be clear. We are advocating for the limited use of biometric security screening only for those who have opted in to provide this information to DHS.

If we do not use this as an opportunity to modernize REAL ID requirements, expand trusted traveler programs, and improve biometrics, we will all spend the next year simply trying to meet the policies of the last decade rather than preparing for the next generation of secure and efficient travel.

There is a major opportunity to modernize the systems DHS sought to strengthen with REAL ID 14 years ago.

I would like to thank the Committee for its leadership to ensuring secure, efficient travel for all Americans. U.S. Travel and our industry look forward to working with you on this issue.

[The prepared statement of Ms. Barnes follows:]

PREPARED STATEMENT OF TORI EMERSON BARNES, EXECUTIVE VICE PRESIDENT,
PUBLIC AFFAIRS AND POLICY, U.S. TRAVEL ASSOCIATION

Chairman Sullivan, Ranking Member Markey, members of the Subcommittee . . . good morning.

I'm Tori Barnes, Executive Vice President of Public Affairs and Policy for the U.S. Travel Association. Thank you for inviting our association, the voice of the broader travel industry, to participate in this important hearing.

U.S. Travel is the only association that represents all sectors of the travel industry—hotels, airports, state and local tourism offices, car rental companies, theme parks and attractions, and many others. With such a diverse membership, our association has a focused mission: to increase travel to and within the United States, while maintaining the highest standards of security.

In 2018, domestic travelers spent \$933 billion in the United States, representing 86 percent of total travel expenditures. Domestic travel spending directly supported 7.7 million American jobs.¹ Travel is vital to the American economy and workforce, and some of the best programs we have to facilitate travel are also ones that strengthen security the most.

And that's what I would like to speak with you about today—to discuss ways we can improve security and efficiency ahead of the October 1, 2020 deadline for REAL ID enforcement.

The REAL ID Act was passed in 2005, and its full implementation has been put off by a series of extensions intended to give states time to bring their IDs into compliance.² Now, the Department of Homeland Security (DHS) has said the days of REAL ID delays is over, and every American will need a REAL ID license or an acceptable alternative—such as a U.S. passport, a U.S. military ID, an enhanced driver's license or a DHS trusted traveler card—to fly next October.³

But Americans simply are not REAL ID ready.

U.S. Travel commissioned Longwoods International, a market research consultancy, to conduct two surveys measuring both the public's understanding of REAL ID Act requirements and awareness of the October 1, 2020 enforcement deadline. The studies, which were fielded in July and September 2019, found that an estimated 182 million Americans (72 percent) say they do not have a REAL ID license or are unsure if they do, and 57 percent of Americans are unaware of the October 1, 2020 deadline for REAL ID enforcement.

In fact, according to our survey, an estimated 99 million Americans (39 percent) say they do not currently have any acceptable form of identification (such as a REAL ID license, U.S. passport, a U.S. military ID, an enhanced driver's license or a DHS trusted traveler card) that can be used to fly starting October 1, 2020. This finding is especially concerning, since, according to the Transportation Security Administration (TSA) and DHS, travelers that arrive at the airport without a REAL ID or an acceptable alternative will be turned away from the checkpoint and not be allowed through security to board their flights.

U.S. Travel Association economists estimate that if the REAL ID deadline were implemented today, approximately 78,500 American travelers would be denied boarding on the first day. This would cost the U.S. economy over \$40.3 million in lost travel-related spending.

If that trend were to continue for a week, 549,500 million travelers would be turned away, costing nearly \$282 million in lost spending.⁴ This is simply unacceptable.

To help solve this problem, the U.S. Travel Association launched an industry-wide public education campaign to increase awareness of the October 1, 2020 deadline for REAL ID enforcement and to encourage Americans to get a compliant driver's license or acceptable alternative before next October.

But we can't solve this by simply pushing people to the DMV. Especially when two states, Oregon and Oklahoma, are not yet issuing REAL IDs and aren't expected to begin until next summer.⁵

REAL ID represented the most secure form of identification when it was conceived in 2005, but technology has advanced greatly in the past 14 years. There is an opportunity to bring security into the future, rather than just working to meet

¹ https://www.ustravel.org/system/files/media_root/document/Research_Fact-Sheet_Domestic_Travel.pdf

² <https://www.dhs.gov/state-extensions>

³ https://www.ustravel.org/sites/default/files/media_root/document/REALID_Infographic.pdf

⁴ https://www.ustravel.org/sites/default/files/media_root/document/REALID_SurveyFindings.pdf

⁵ <https://www.dhs.gov/real-id>

the requirements of the past. In order to take advantage of this opportunity, Congress and the administration must act.

U.S. Travel has outlined four policy proposals to modernize security and avoid chaos at our airports come October 1, 2020.⁶

First: Turning travelers away at the checkpoint is not an option. Congress should immediately direct the TSA to work with the private sector to develop procedures for clearing travelers that do not have a REAL ID or acceptable alternative on October 1, 2020. In particular, rural airports with limited resources and infrequent air travelers need to have procedures in place to securely screen travelers who are not REAL ID ready. DHS and TSA should leverage existing airport infrastructure, services and identification methods to provide a solution for passengers who are unable or unaware of the need to obtain a REAL ID driver's license or accepted alternative.

Second: Congress must immediately direct DHS to utilize the existing security and identification features of trusted traveler programs by designating TSA Precheck and CLEAR enrollment as acceptable alternatives to REAL ID licenses. This process should be in place no later than October 1, 2020. Enrollees in TSA Precheck, for example, must be vetted against several law enforcement databases, ensuring greater security than a REAL ID alone.

Third: Congress must immediately act to modernize the REAL ID Act to allow for mobile devices and web-based REAL ID applications, and to permit TSA to accept mobile or digital REAL ID-compliant driver's licenses.

The REAL ID Act of 2005 (49 U.S.C. § 30301 Note) and Federal regulations governing state implementation (6 CFR Part 37) require first-time applicants to apply in person at a DMV and present physical, rather than electronic, documents for verification. The in-person application requirements stem from statutory language directing the "presentation and verification" of source documents that DHS interprets to mean in-person transactions using physical documents. The REAL ID Act directive for states to complete a "mandatory facial capture" is also interpreted by DHS to mean an in-person transaction at a physical DMV location.

Modernizing the law and regulations will reduce DMV backlogs and increase security checkpoint efficiency. In 2005 there was no TSA Precheck and no mobile boarding passes—advances in technology have allowed for greater security than America had when the law was enacted.

Fourth: DHS should accelerate the implementation of biometric identity verification technology at TSA checkpoints. This is simply a way to provide faster, more secure screening, using information that trusted travelers and passport holders have already provided to DHS. This is what TSOs are already doing—verifying an ID matches the person in front of them. Biometric identity verification does the exact same thing, but more accurately, securely and quickly. CBP is already using this technology in the Entry/Exit process. DHS should align with Customs and Border Protection (CBP) and move this technology to the TSA screening line to verify the identities of travelers who opt in.

Let me be clear: When it comes to biometrics, we are advocating for uses that are:

- Opt-in, where Americans have already decided to provide their information to DHS, the U.S. Department of State or a trusted traveler program;
- Governed by clear and reasonable guidelines for accuracy, privacy and performance; and
- Already being pursued by DHS at the direction of Congress, such as biometric exit, registered traveler, and the PreCheck biometric pilot program.

We are asking Congress to prioritize the opt-in programs that already have millions of participants; direct DHS to issue clear rules for accuracy, privacy, and performance as soon as possible; and align TSA's implementation of biometrics for passport holders and Precheck enrollees with DHS goals for implementing biometric exit.

If we don't use this as an opportunity to modernize REAL ID requirements, expand trusted traveler programs and enhance and improve biometrics, states, Congress, DHS and the traveling public will spend the next year simply trying to meet the policies of the last decade, rather than preparing for the next generation of secure and efficient travel.

There is a major opportunity to modernize the systems DHS sought to strengthen with REAL ID 14 years ago. I'd like to thank the Committee for its leadership in ensuring secure, efficient travel for all Americans. U.S. Travel and our industry looks forward to working with you on this issue.

⁶https://www.ustravel.org/sites/default/files/media_root/document/REALID_Factsheet_UST.pdf

Thank you.

REAL ID SURVEY

SUMMARY OF FINDINGS

Survey conducted by
Longwoods
INTERNATIONAL

The vast majority of Americans do not have or are confused about REAL ID driver's licenses¹

- ★ **87%** of American adults say they have a state-issued driver's license, making it the most commonly held and important form of identification for commercial air travel
 - 53% say they have a U.S. passport or passport card (second highest response)
 - Only 9% say they have a DHS trusted traveler card
- ★ Only **16%** of Americans believe they have a REAL ID license and can correctly identify the star
 - 44% of Americans believe their state-issued driver's license is a REAL ID
 - 16% said they were certain because a star appeared in the upper righthand corner of their license (which is the best indicator of a REAL ID)
 - 14% said they were informed by the DMV, but did not also select the star
 - The remaining respondents cited reasons which indicate they are either incorrect or may be confused, including:
 - 5% who said they were certain because a microchip appeared on their license
 - 3% who said they were certain because an American Flag appeared on their license
- ★ In total, an estimated **182 million Americans² (72%)** say their driver's license is not a REAL ID or they may be confused
 - 21% say they are certain their license is not a REAL ID
 - 23% say they are unsure if their license is a REAL ID
 - 28% believe their license is a REAL ID but did not correctly identify the star

Nearly 2-in-5 Americans say they do not have any form of REAL ID compliant documents³

- ★ An estimated **99 million Americans⁴ (39%)** say they do not have any form of identification that will be accepted starting October 1, 2020
- ★ **61%** of Americans say they have at least one form of REAL ID-compliant documents
 - 16% say they have a state-issued REAL ID (and correctly identified the star)
 - 39% say they have a passport, but do not have a state-issued REAL ID or are unsure whether their driver's license is a REAL ID
 - 6% that have some other form of REAL ID-compliant identification, but no state-issued REAL ID or passport
- ★ Of the **60%** of Americans who say they are planning to fly in the next two years
 - Only 18% are certain they have a state-issued REAL ID and correctly identified the star
 - 62% have a passport or some other federally approved identification, but either do not have a REAL ID or are uncertain if their driver's license is REAL ID compliant
- ★ Only **42%** of passport holders say they typically carry their passports with them when traveling domestically by air⁵

REAL ID SURVEY

SUMMARY OF FINDINGS

Most Americans are unaware of the October 1, 2020 deadline for air travel⁶

- ★ Only **43%** of Americans are aware that as of October 1, 2020 they will be required to present a REAL ID-compliant document at TSA checkpoints
- ★ **57%** of Americans are unaware of the October 1, 2020 REAL ID deadline for air travel, including:
 - 30% who said they don't know or are unsure about a REAL ID deadline
 - 9% who believe a REAL ID will be required for purchasing a firearm
 - 5% who believe a REAL ID will be required for registering a vehicle with the DMV

Most Americans support government action to mitigate challenges posed by REAL ID Implementations⁷

- ★ When asked what steps, if any, should be taken to address challenges posed by REAL ID implementation, **70%** of Americans said they support some kind of leniency for travelers without REAL ID driver's licenses or acceptable alternatives
- ★ Only **29%** believe the deadline should be enforced without any exceptions
- ★ Alternatives include:
 - Providing an additional short-term grace period
 - Allowing those without a REAL ID to pass through, but with additional personal and baggage screening
 - Allow short-term exemptions for travelers who begin enrollment in Precheck

If Americans fail to obtain proper identification ahead of October 1, 2020, the disruption to air travel could have a significant impact on the U.S. economy⁸

- ★ If REAL ID enforcement were implemented today, an estimated **78,500 travelers** could be turned away on the first day, resulting in **\$40.3 million** (excluding airfares) in **lost travel spending** on the first day.
- ★ If this daily impact lasted a week, an estimated **549,500 air travelers** could be turned away in the first week, costing travel businesses nearly **\$282 million in lost spending**.

REAL ID SURVEY

SUMMARY OF FINDINGS

METHODOLOGY

To help quantify the challenges posed by REAL ID implementation, the U.S. Travel Association commissioned Longwoods International, a market research consultancy, to conduct two surveys measuring public's understanding of REAL ID identifications and the October 1, 2020 enforcement deadline for commercial air travel.

The July 2019 survey was an online self-completion survey fielded July 9 through 12, 2019 using a national sample randomly drawn from Dynata's consumer panel of 1,000 adults, ages 18 and over. The results were weighted at tabulation to correct for differences between the observed sample and the sample universe using the most recent Census targets for age, gender, income, household composition and region. The survey has a margin of error +/-3% at 95% confidence level.

The September 2019 survey was an online self-completion survey fielded September 4 through 6, 2019 using a national sample randomly drawn from Dynata's consumer panel of 1,000 adults, ages 18 and over. The results were weighted at tabulation to correct for differences between the observed sample and the sample universe using the most recent Census targets for age, gender, income, household composition and region. The survey has a margin of error +/-3% at 95% confidence level.

1. July 2019 Longwoods International Survey
2. Analysis by U.S. Travel Association
3. July 2019 Longwoods International Survey
4. Analysis by U.S. Travel Association
5. September 2019 Longwoods International Survey
6. September 2019 Longwoods International Survey
7. September 2019 Longwoods International Survey
8. Analysis by U.S. Travel Association

U.S. TRAVEL
ASSOCIATION

1100 New York Avenue, NW Suite 450 Washington, D.C. 20005 | TEL 202.408.8422 | ustravel.org

Senator SULLIVAN. Thank you, Ms. Barnes.
Mr. McLaughlin.

**STATEMENT OF CHRIS McLAUGHLIN, CHIEF OPERATIONS
OFFICER, DENVER INTERNATIONAL AIRPORT**

Mr. McLAUGHLIN. Chairman Sullivan, Ranking Member Markey, members of the Subcommittee, Senator Gardner, thank you for your continued leadership on aviation security and for inviting me to this important hearing. I look forward to sharing an airport perspective on the importance of enhancing aviation security.

I am particularly grateful to testify at today's hearing because aviation and airport security has been a career-long passion. Over the past 20 years, I have worked in nearly every sector of our industry, including for airlines where I ran ground operations, for the TSA as the Federal Security Director for Colorado, and in D.C. where I led the initial deployment of TSA's PreCheck program as the Assistant Administrator for Security Operations. And most recently I worked for two disruptive technology companies helping them to gain traction in commercial aviation security.

This morning, I would like to focus on the importance of continued innovation in aviation security, with specific regard to security modernization, continued focus on TSA PreCheck, and the implementation of REAL ID.

Innovation in aviation security is critical for three main reasons. First and foremost, we must stay ahead of an adaptive and committed adversary. Second, we must keep up with ever-increasing passenger volumes. And third, airports must maintain the autonomy to flex to our unique customer needs and preferences.

As threats to aviation have evolved, DEN has been proactive. Notably, we have begun to overhaul our main terminal in a way that strengthens the public area without compromising its iconic nature. In response to attacks in pre-security airport locations, we are repositioning our checkpoints to more quickly disperse and insulate our passengers.

We have worked with the TSA to explore innovations to bring this vision to life. Soon we will roll out TSA's CT program. Earlier we were among the first airports in the Nation to install automated screening lanes. And last fall, we became the first to permanently install a new generation body scanner that is more natural, less invasive, and faster than traditional systems.

While keeping security top of mind, we also remain keenly aware of our passenger volumes. Currently the fifth busiest airport in the country, DEN is experiencing exceptional growth. We will hit nearly 70 million passengers this year.

New technologies get us closer to meeting our passenger demand, but technology alone is not enough. TSA PreCheck, for example, has succeeded at improving the screening process for its members. However, low enrollment has delayed the ultimate goal of improving security and processing time for all passengers. TSA must advance PreCheck, and the best way to do this is through initiatives specified in the TSA Modernization Act.

Recognizing that robust identity verification fortifies risk-based security, DEN supports the implementation of REAL ID, and we are committed to doing our part to ensure the traveling public is

well informed before they get to the checkpoint. We also believe that the voluntary use of biometrics can complement REAL ID.

Clearly, our need to stay ahead of the next threat, coupled with our passenger growth, has impacted our identity as an airport. It is with this in mind that we sought to expand, to re-imagine, and to modernize our checkpoints. We are doing our part, and TSA has made some progress, especially in formally developing their gifting policy.

That said, the process should be easier and, frankly, it should be less expensive. We are making substantial investments in order to deliver our future checkpoint. DEN is buying the equipment. We are paying for the installation. We are paying to remove and store the existing equipment, and we are funding a 4-year maintenance plan. We are not doing this because we agree that local jurisdictions should finance the Federal security system. We are doing it because our customers cannot afford to wait.

Two years ago, our CEO, Kim Day, offered this Committee two actions that Congress could take to address the funding needed to modernize security.

First, Congress should discontinue diverting the 9/11 security fee. Last fiscal year, \$1.4 billion of security fees were diverted away. In fact, billions of dollars that could have gone to testing and deploying innovative technology have instead gone to pay down unrelated government activities since the law was changed in 2013.

The second is the passenger facility charge, or the PFC. Even a modest increase in the PFC would give airports the flexibility to prioritize security efforts to match passenger growth.

Both these ideas remain valid today.

I am grateful for the opportunity to testify in front of the Subcommittee, and I am confident that with your leadership we can capitalize on real opportunities to make travel safer and more efficient. Thank you.

[The prepared statement of Mr. McLaughlin follows:]

PREPARED STATEMENT OF CHRIS McLAUGHLIN, CHIEF OPERATING OFFICER,
DENVER INTERNATIONAL AIRPORT

Chairman Sullivan, Ranking Member Markey, and members of the Subcommittee, thank you for your continued leadership on aviation security and for inviting me to this important hearing. My name is Chris McLaughlin, and I am the Chief Operating Officer of Denver International Airport (DEN). Security is a critical focus for airport operators, and I look forward to sharing an airport perspective on the continued importance of enhancing aviation security.

I would also like to thank Senator Gardner, who serves on the full committee, for continuing to be a great champion for Colorado and Denver's airport. His leadership in fostering innovation and driving forward-looking security solutions at our Nation's airports has resulted in increased efficiency and security for the traveling public.

I am particularly grateful to testify in today's hearing because aviation and airport security has been a career-long passion of mine. Over the past twenty years, I have worked in nearly every sector of our industry. I worked for two airlines where I ran ground operations at both the hub and system level; for the TSA, where I served as the Federal Security Director for Colorado, and here in D.C. as the assistant administrator for security operations. In that role, I oversaw all ~450 U.S. airports. I also played a leadership role in the development and deployment of TSA's PreCheck program. Prior to joining the airport, I served in executive roles for two disruptive technology companies, helping them to gain traction during the early phases of their growth in commercial aviation security.

This morning, I would like to focus my remarks on the importance of continued innovation in aviation security, with specific regard to a few key areas: the need to modernize our security infrastructure and the acquisition challenges associated with doing so, continued focus on important programs like TSA PreCheck, the implementation of REAL ID, and advancements in biometric technology. I know these issues are important to the Subcommittee, and I would like to convey how important they are to airports as well.

Innovation in aviation security is critical for three main reasons. First and foremost, we must stay ahead of an adaptive and committed adversary. Second, we must keep up with ever increasing passenger volumes—from infrastructure to operations. And third, airports must maintain the autonomy to differentiate ourselves according to our unique customer needs and preferences.

As threats to aviation have evolved, Denver has proactively responded to the changing landscape, making a point to partner with Department of Homeland Security agencies and airlines on innovations that enhance security. Perhaps most publicly, we have embarked on a project to overhaul our main terminal in a manner that strengthens our public area security posture without compromising its iconic nature. Largely in response to attacks in pre-security areas like Brussels and Istanbul, and domestic incidents like those at Fort Lauderdale and LAX, Denver is repositioning our checkpoints in a manner that more quickly disperses and insulates our passengers.

From the beginning of our planning process, we have worked diligently with TSA to explore potential innovations that allow TSA officers to focus on security at the checkpoint—rather than crowd control.

- We partnered with TSA in 2017 to pilot a palm-print biometric authentication technology.
- We were among the first airports in the Nation to install Automated Screening Lanes, and because of the positive results we have seen, we are planning our next phase of installations now.
- We are among the first group of airports selected for TSA’s CT program and will soon be installing six lanes at DEN.
- Last but not least—having served as the Federal Security Director for TSA when AIT was first deployed a decade ago—I am grateful that last fall DEN became the first airport in the Nation to install a new generation of body scanning technology that is more natural, less invasive, and faster than traditional systems.

While our primary objective in this project has been to improve security, we have remained keenly aware of our growth in passenger traffic as well. Currently the 5th busiest airport in the country and 20th in the world, Denver is experiencing exponential growth. We eclipsed 60 million passengers served in 2017, and just two years later, we will serve nearly 70 million travelers this year.

Each of the technologies that I mentioned gets us closer to meeting our passenger demand. In addition to these, it is critical that TSA continue to advance its risk-based security initiatives. TSA PreCheck has succeeded in its goal of enhancing security and improving the screening process for individuals enrolled in the program. However, the low overall enrollment rate has prevented TSA from achieving its ultimate goal of improving security and processing time for all passengers. TSA must continue to advance the PreCheck program and it is my belief that the best way to do this is through the third-party initiatives specified in the TSA Modernization Act.

Recognizing that robust identity authentication and verification is a critical component of risk-based security, DEN supports the upcoming implementation of REAL ID and we are committed to doing our part to ensure the traveling public is well informed and prepared before they get to the checkpoint. Similarly, we believe that the *voluntary* use of biometrics improves the passenger experience for some while strengthening security for all. We support guardrails to protect the privacy of the traveling public. Still, based on existing aviation programs and consumer trends in other areas, it is likely that a growing number of passengers will voluntarily submit their biometrics in order to expedite their security screening process. By verifying these passengers’ identity faster, officers have more time to verify remaining passengers using traditional means.

While it may not be clear that “individualism” is something that should be considered at a hearing on security, our identity is something that we take very seriously at DEN. We are proud to have been recognized as the top U.S. airport by Skytrax and The Wall Street Journal this past year. Yet, at least for The Journal, we achieved this ranking despite finishing 17th out of the top 20 airports for our overall

security experience. This score is not a reflection on the hard work or customer focus of our TSA partners. Rather it reflects checkpoints that need to be expanded, re-imagined, and modernized. As I said earlier, we are doing our part, and TSA is working with us.

We appreciate TSA's effort in developing its gifting policy and for issuing an approved list of automated screening lane vendors this year. And we applaud the deliberate work the agency has undertaken to test new technology and ensure our security remains the highest priority. That said, it feels like the process should be easier, and frankly, less expensive for airports.

We are making substantial financial investments in order to deliver a checkpoint with modern technology. DEN is buying the equipment, paying for its installation, paying to remove and store existing equipment, and—under the new gifting program—funding a four-year maintenance plan. After which, we will be “allowed” to give the equipment to TSA. We are not alone in this. Other local jurisdictions as well as airlines are making similar investments. We're not doing this because we believe we should. We're doing it because our customers can't afford for us to wait.

There is growing concern across the industry that the aviation community's willingness to lend a hand after long TSA lines created a perceived crisis in the summer 2016, is drifting into an expectation that local jurisdictions will finance the Federal security system.

Two years ago, our CEO Kim Day came before this Committee and offered two ideas Congress could authorize to address the funding needed to modernize security and keep pace with the exceptional growth in air travel:

First, Congress could discontinue the practice of diverting the 9/11 security fee revenues to non-security purposes. In Fiscal Year 2019 alone, \$1.4 billion of the fees air travelers paid for security were diverted away. In fact, billions of dollars that could have gone to testing innovative technology and recapitalizing checkpoints have instead gone to pay down unrelated government activities since the Balanced Budget Agreement of 2013 was signed. And, billions of future resources will similarly be diverted unless Congress addresses this situation.

The second is the Passenger Facility Charge, or PFC. Even a modest increase in the PFC on originating and destination passengers would give airports the flexibility to prioritize security efforts to match the growth we are seeing.

Both ideas remain valid today.

I am grateful for the opportunity to testify in front of the Subcommittee today. I am confident that with your leadership—and the work of our stakeholders represented here at this witness table—that we can capitalize on real opportunities to make travel safer and more efficient.

Thank you. I look forward to your questions.

Senator SULLIVAN. Thank you, Mr. McLaughlin.

And the next witness, Ms. Beyer.

STATEMENT OF LAUREN BEYER, VICE PRESIDENT, SECURITY AND FACILITATION, AIRLINES FOR AMERICA

Ms. BEYER. Good morning, Chairman Sullivan, Ranking Member Markey, and members of the Subcommittee.

My name is Lauren Beyer, and I am the Vice President for Security and Facilitation at Airlines for America. Thank you for inviting me here today to discuss aviation security.

As an industry, the safety and security of our passengers and employees is our single highest priority. We recognize the sometimes challenging security environment when operating all over the world, and these challenges have grown in recent years to include cybersecurity and unmanned aircraft systems. We are dedicated to working cooperatively and collaboratively with TSA and other partners to confront these challenges.

U.S. airlines strongly advocate for the development of pragmatic, risk-based, and outcome-focused security measures. Such an approach provides a framework that is more agile and more responsive to threats and allows TSA and industry to focus resources on the highest risks.

We must continue to build a partnership with TSA that is collaborative and proactive. We have made good progress in this regard under Administrator Pekoske's leadership, and we appreciate the administrator's steadfast commitment to making consistent coordination with industry part of the agency's culture and standard way of doing business. Coordination is key to security.

I would also like to thank this Committee for the monumental achievement of enacting the TSA Modernization Act last year. Many of the provisions in that bill were critical security initiatives for airlines. We continue to urge TSA to expeditiously and fully implement those provisions that are outstanding, and we respectfully request this subcommittee continue oversight of timely implementation. A few provisions to note.

We are pleased that TSA has established an air cargo security office in accordance with the Act. Consolidation of air cargo expertise and decisionmaking within TSA will be hugely beneficial to provide focus, momentum, and clear guidance on cargo security initiatives. We have already seen progress through TSA's successful rollout of the Third-Party Canine Program, and we continue to work with TSA on efforts to advance additional technological resources for the screening of air cargo.

We are also in strong support of the innovation provisions in the Act, and we encourage TSA to focus on expediting the resourcing and permanent rollout of successful innovation pilots so that these efforts are seen through from idea to completion.

Insider threat continues to be of great concern to the aviation industry. U.S. airlines are committed to working proactively with TSA, the FAA, and other industry partners to mitigate this continuing challenge. In fact, A4A, along with our stakeholder partners, hosted an event earlier this year to solicit insider threat best practices.

We are also an avid supporter of and participant in the Aviation Security Advisory Committee's Insider Threat subcommittee.

While not part of the TSA Modernization Act, I would also like to emphasize and voice some concern regarding the October 1, 2020 REAL ID enforcement deadline for boarding commercial aircraft. U.S. airlines have been working closely with DHS and TSA to amplify their messaging. Since DHS and TSA have not indicated any willingness to extend the deadline, we are committed to keeping up the momentum to educate travelers. However, much needs to be done within the next year for a smooth transition. We appreciate Chairman Wicker's leadership in raising awareness of REAL ID requirements and look forward to working with the Committee on this issue.

Finally, two points on funding.

First, this Committee knows well that a portion of the aviation security fees are diverted to our general deficit reduction every year. We continue to request Congress redirect TSA passenger security fee revenue back to aviation security. And we appreciate Ranking Member Markey and Senator Blumenthal's leadership on this issue and their legislation eliminating the diversion.

Second, I would be remiss not to mention and emphasize the importance of operational stability and predictability for the TSA during any lapse in funding. The airline industry is reliant upon the

TSA providing critical security services. We implore all involved to make sure budgetary contingency plans are in place to allow TSA to operate normally if a shutdown caused by a lack of funding occurs.

Thank you. I appreciate the opportunity to testify and look forward to any questions.

[The prepared statement of Ms. Beyer follows:]

PREPARED STATEMENT OF LAUREN BEYER, VICE PRESIDENT, SECURITY AND FACILITATION, AIRLINES FOR AMERICA

Good morning Chairman Sullivan, Ranking Member Markey, and members of the Subcommittee. My name is Lauren Beyer, and I am the Vice President for Security and Facilitation at Airlines for America (A4A). Thank you for inviting me here today to discuss aviation security.

Overview. The safety and security of our passengers and employees is our single highest priority. We recognize the sometimes-challenging security environment when operating in more than 800 airports in nearly 80 countries, and these challenges have grown in recent years to also include cybersecurity and unmanned aircraft systems. We are dedicated to working cooperatively and collaboratively with the Transportation Security Administration (TSA) and other partners around the world every day to keep our skies safe and secure.

Securing the aviation system protects people first and foremost, but it also helps preserve the American economy. The U.S. airline industry helps drive \$1.5 trillion annually in U.S. economic activity and supports more than 10 million U.S. jobs. When talking about the daily challenges of aviation security it is important to understand the depth and magnitude of what takes place and what is transported by air: U.S. airlines carry 2.4 million passengers and more than 58,000 tons of cargo every single day. The National Strategy for Aviation Security (NSAS) published in December of last year underscores this dual objective:

“The NSAS aims to enhance the safety and security of the Aviation Ecosystem, preserving the freedom of operations for legitimate pursuits and facilitating American prosperity.”¹

Given the vast geography and sheer volume of air travel it is exceedingly important that we approach security in a smart, effective, and efficient manner that best utilizes the finite resources available to both improve security and facilitate commerce. This becomes even more imperative given the expectation that both passenger and cargo traffic are expected to grow in the coming years.

Indeed, the 2019 summer travel season was the busiest ever with TSA screening 262 million passengers and crew between May 22–September 3. This equates to an almost 3.4 percent increase over last year. Overall, TSA performed well during this critical season, and I would like to thank TSA for addressing the growing volume of passengers and cargo with increased staffing and overtime allocation.

Risk-Based Security. As an industry, we believe aviation benefits most from the principles of risk-based security—which is the lynchpin and bedrock of our security system today. A risk-based approach recognizes that “one size fits all” security is not the optimum response to threats. The implementation of risk-based, outcome-focused measures has been a widely accepted approach to aviation security by governments and industry alike for some time. We know the effectiveness of risk-based security and we therefore strongly support it.

One of our Nation’s greatest challenges is to strike the right balance when managing risk. Enhanced aviation security and the efficient facilitation of passengers and cargo are not mutually exclusive goals; government and industry must continue to work together to find pragmatic approaches that appropriately balance these goals.

By utilizing and following risk-based principles we provide a security framework that is more agile and more responsive to current and emerging threats and allows TSA and industry to focus resources on the highest risks. This framework also takes the operational complexity of the U.S. aviation system into account.

Key to our effort to develop and effectively implement risk-based security measures is coordination between TSA and industry. We must continue to build partnerships between TSA and industry that focus on pursuing security improvements in

¹ <https://www.whitehouse.gov/wp-content/uploads/2019/02/NSAS-Signed.pdf>

a collaborative and proactive manner. Congress emphasized the importance of this partnership throughout the *TSA Modernization Act of 2018*.

Published last year, the TSA Administrator's Intent which sets out how TSA intends to execute its strategy through the end of 2020 specifically directs the agency through its guiding principles to "actively seek stakeholder input" and to "collaborate to drive value . . . through action, transparency and accountability." Further, the first strategic priority is to improve security, including through "consistent communications and coordination with regulated and non-regulated partners."² We have made good progress in this regard under Administrator Pekoske's leadership, and U.S. airlines appreciate the Administrator's steadfast commitment to making *consistent coordination and collaboration with industry* part of the agency's culture and standard way of doing business.

TSA Modernization Act. I would like to thank this Subcommittee and the Congress for the monumental achievement of enacting the *TSA Modernization Act*, the first reauthorization of TSA in its 18-year existence. Many of the provisions in this bill were important to our membership to move critical security initiatives forward. One such provision was the establishment of a 5-year term for the TSA Administrator. The continuity and stability that a 5-year term will bring to a still young agency that has experienced tremendous leadership turnover is much needed.

A4A and airlines have met with TSA periodically since the bill's passage to review implementation status. While we recognize the volume of requirements placed on TSA by the bill and in some cases the short deadline required, we continue to urge TSA to expeditiously and fully implement those provisions that are outstanding. We respectfully ask this Subcommittee to do the same.

A4A has also partnered with TSA directly or through our participation on the Aviation Security Advisory Committee (ASAC) to provide input on TSA's execution of several provisions. One example of this partnership is the provision that requires an airport worker access controls cost and feasibility study. For TSA to assess the impact of employee screening including a comparison of estimated costs and effectiveness to TSA, airports, and airlines, it necessarily requires close coordination with industry to ensure the full scale of potential impact is considered.

Several cargo-related provisions of the *TSA Modernization Act* deserve mention. We are pleased that TSA has established an air cargo security office within TSA Policy, Plans and Engagement. Consolidation of air cargo expertise and decision-making within TSA will be hugely beneficial to provide focus, momentum and clear guidance on critical cargo security initiatives, including those based on recommendations from the ASAC Air Cargo Subcommittee. We have already seen progress through TSA's successful rollout of the Third-Party Canine Program. We continue to work with TSA on efforts to advance additional technological resources for the screening of air cargo and hope to see additional progress in the coming year.

Innovation in aviation security is key to ensure we continue to stay ahead of adversaries, and innovation frequently has the added benefit of improving the customer experience. This is a primary reason we support TSA's Innovation Task Force (ITF). We encourage TSA to now shift their focus to expediting the resourcing and permanent rollout of successful ITF pilots so that these efforts are seen through from idea to completion.

Additionally, A4A supports TSA's evaluation of biometrics for identity verification at the security checkpoint as well as the consultation with U.S. Customs and Border Protection (CBP). The primary benefit of the biometric program is the enhanced ability to protect against identity fraud, but we also believe it enhances customer experience.

A4A members have worked closely with TSA and CBP during this process. While we believe the privacy protections currently in place are effective, we will continue to work with TSA and our passengers to ensure the highest levels of privacy. Airlines already collect and transmit biographic data to the Department of Homeland Security (DHS) to comply with Federal security requirements, so we have experience in the area. Airlines, like DHS, also have committed to strict privacy principles as it relates to the use of biometric information. For facial recognition technology, these principles include opt-out options and non-retention of photos for business purposes. We all agree that privacy is of the utmost importance.

REAL ID. Effective October 1, 2020, travelers will be required to have a REAL ID compliant driver's license or alternate approved identification to pass through TSA checkpoints at airports, the final enforcement deadline of the *REAL ID Act of 2005*.

We appreciate Chairman Wicker's leadership in raising awareness of REAL ID in recent hearings and the media about the potential disruption to air travel next year

²https://www.tsa.gov/sites/default/files/tsaadminintent_2018.pdf

for those passengers who are not prepared with a compliant driver's license or other form of identification.

U.S. airlines have been working closely with DHS and TSA to amplify their messaging and to direct travelers to the appropriate websites to ensure they're educated about how to obtain a REAL ID compliant identification card. To that end, A4A participated in the TSA's press conference on October 1, along with other coalition partners, to highlight our public awareness campaigns.

Over the last year, we have undertaken a variety of activities to highlight this issue. For example, our coalition wrote the states' governors asking them to join us in making the public more aware of the upcoming deadline. Since consumers in many states still have the choice between a non-compliant ID, the states need to play a key role in ensuring that consumers understand that even some new IDs may not be compliant. We also asked the governors to consider revising communications to their residents to make clear the difference between REAL ID compliant and non-compliant IDs.

U.S. airlines also are employing a variety of methods to prominently share information such as posting notices of the upcoming change on their websites and social media, deploying videos on their in-flight entertainment systems in addition to putting the message in in-flight magazines.

Since DHS and TSA have not given any indication of a willingness to extend the deadline, we are committed to keeping up the momentum in educating the public in order to ensure that the 2.4 million people who travel every day will be able to flow through the system as seamlessly as possible.

Insider Threats. Insider threat continues to be of great concern to the aviation industry, and incidents in recent years are a reminder of the constant vigilance required to keep our skies safe. U.S. airlines are committed to working proactively with TSA, the Federal Aviation Administration and other industry partners to mitigate this continuing challenge. In fact, A4A along with many of our stakeholder partners hosted an event earlier this year that brought together subject matter experts from across the industry and government to solicit airport and aircraft security best practices. These practices were shared across U.S. aviation industry stakeholders. We are currently working with TSA and our other stakeholder partners to determine the best mechanism to continue such voluntary sharing of best practices, whether that be an insider threat information-sharing platform or an ongoing industry-wide working group.

A4A is also an avid supporter of and participant in the ASAC, including its Subcommittee on Insider Threat. We strongly believe the ASAC is the best venue in which to examine and produce recommendations on insider threats and other security matters. The ASAC includes representatives from across the aviation industry and is the traditional mechanism through which TSA and industry collaborate to develop the most effective aviation security measures. The ASAC is a tried, tested and proven mechanism to provide the TSA Administrator diverse stakeholder input and sound security recommendations that achieve the objective of enhanced security while maintaining respect for and flexibility that accommodates the complexity of the U.S. aviation system. This fact is recognized both by Congress through the numerous provisions of the *TSA Modernization Act* that require consultation with or recommendations from the ASAC as well as the TSA through their strong history of acceptance of ASAC recommendations and the recent establishment of a similar committee for surface transportation stakeholders.

Stop the annual practice of diverting passenger security fee revenue. U.S. aviation and its customers are subject to 17 Federal aviation taxes and 'fees'. Included within those numbers are revenues that are intended to support activities at the TSA, including the September 11th TSA Passenger Security Fee. As this Subcommittee knows well, that 'fee' is \$5.60 imposed per one-way trip on passengers enplaning at U.S. airports with a limit of \$11.20 per round trip; the fee also applies to inbound international passengers making a U.S. connection.

However, starting in Fiscal Year 2014, Congress started diverting a portion of that fee toward general deficit reduction and is scheduled to continue diverting these critical resources through Fiscal Year 2027. From our perspective, this policy is simply unacceptable. Airlines and their customers now pay \$1.8 billion more in TSA security fees—\$4.1 billion (2018) vs. \$2.3 billion (2013)—for the exact same service. The concept of a 'fee' specifically charged to pay for a specific service has long been lost in our industry and they have all simply become taxes by another name. We would respectfully request this Committee do everything in its power to redirect TSA passenger security fee revenue back where it belongs: paying for aviation security. These diverted funds could go a long way to increase TSA capacity and capability to mitigate risk.

We appreciate Ranking Member Markey and Senator Blumenthal's leadership on this issue through introduction of legislation to eliminate the diversion of security fees.

TSA Funding. I would be remiss not to mention and emphasize the importance of operational stability and predictability for the TSA during times of government shutdown caused by a lack of appropriation. The airline industry is reliant upon the TSA providing critical security services; simply, they are essential to our operations. Even minor variations in staffing levels can have dramatic impacts on wait times. Shutdowns come in various forms and circumstance. However, they all have one common thread in that they quickly expose the critical role our government professionals play in many aspects of our lives that we simply take for granted as standard operating procedure. We implore all involved to make sure budgetary contingency plans are in place to allow TSA to operate normally if a shutdown caused by lack of funding occurs. We welcome the Committee's support in the development and implementation of practical and agreeable solutions that would mitigate or alleviate any future shutdown scenarios. We believe the traveling and shipping public deserve continuity.

Thank you, we appreciate the opportunity to testify and look forward to any questions.

Senator SULLIVAN. Thank you, Ms. Beyer.
Mr. Cornick.

**STATEMENT OF KEN CORNICK, CO-FOUNDER AND PRESIDENT,
CLEAR**

Mr. CORNICK. Good morning, Chairman Sullivan, Ranking Member Markey, and members of the Senate Commerce Subcommittee on Security.

My name is Ken Cornick. I am the Co-founder and President of CLEAR, a registered traveler company, and I am honored to be here today.

Following the 9/11 attacks, Congress passed the Aviation and Transportation Security Act of 2001. This legislation led to the creation of the Registered Traveler, or RT, program. Congress' goal was to both enhance security and improve the traveler experience. In 2006, under the Federal registry notice, multiple RT providers began operations. Unfortunately, RT providers fell victim to the great recession and in 2008 ceased operations.

Together with my co-founder, Caryn Seidman Becker, we purchased CLEAR's assets in 2010 and relaunched the company as a secure identify platform initially in Orland and Denver airports. We are proud to be an American-owned company with a mission to strengthen homeland security and delight consumers with frictionless experiences.

CLEAR has grown significantly as travelers have recognized the efficiency of our biometric process, and airports have recognized the security, customer service, and economic benefits of adopting CLEAR. By year end, CLEAR will have around 5 million members in 35 of our nation's largest airports. CLEAR processes almost 5 percent of the nation's originating air passengers using biometrics and upwards of 10 percent in the airports in which we operate.

Our secure enrollment platform establishes an impermeable link between one's identity and their biometrics. Our process entails digitally authenticating a traveler's government-issued ID, establishing that the person enrolling is definitively the person on such document through the use of challenge questions driven by commercially available data, and last by capturing biometric data, including fingerprints, iris, and face. The enrollment process takes

approximately 5 minutes. Once completed, the traveler can use CLEAR immediately.

We have had a significant and positive economic impact in the communities in which we operate, as we have created over 2,000 jobs and shared tens of millions of dollars with our airport partners and municipalities through revenue share agreements. Our success is driven by a strong public-private partnership with TSA. This partnership is a win-win for all stakeholders, driving innovation, enhancing security, and efficiency for travelers. CLEAR is a force multiplier for TSA bringing significant additional resources to the checkpoint at no cost to taxpayers.

We fully support TSA's efforts to drive checkpoint efficiency through the introduction of new technology such as biometrics. Further, CLEAR is eager and has offered to invest its own capital, technology, and labor at the checkpoint to support TSA in its mission.

We can and want to do more with TSA. We see many areas for collaboration. We have vast experience in biometrics, credential authentication, biometrics deployment, identity management, and more.

Given today's environment, I think it is really important to address data security, which is core to our business. We have invested significantly in cybersecurity to ensure our systems are best in class. CLEAR is subject to regular TSA audits, and as a result of those investments and TSA's oversight, we have been designated FISMA-High by TSA. That is the highest government cyber compliance rating available.

CLEAR is also SAFETY Act certified by the Department of Homeland Security as a qualified anti-terrorism technology.

In addition to securing our operations and our customers' data, we take the privacy of our members extremely seriously. CLEAR is a 100 percent opt-in service, and we do not sell customer data.

From an operational perspective, our 2,000-plus passionate team members, also known as Ambassadors, are all SIDA-badged and trained on security.

In the past few years, we have forged partnerships with premier travel companies, including Delta Airlines, United Airlines, Hertz, and American Express. With these partnerships, we are delivering seamless and secure traveler experiences from curb to gate. Examples include biometric bag check, lounge entry, boarding, and car rental exit lane.

Beyond the airport, we have a partnership with major league baseball and sports teams to provide biometric ticketing and secure access to over 24 stadiums across the country.

I want to thank the Committee for its ongoing support of the Registered Traveler program and its efforts to ensure it remains an important defense layer in aviation security.

In closing, I ask Congress to support a modernization of the RT program and the resulting public-private partnership that is driving the use of biometrics in aviation security. We have come a long way, but we have more to do. By working with all stakeholders, we know we can continue to support TSA's mission and the goals of improving security while delighting travelers.

Thank you.

[The prepared statement of Mr. Cornick follows:]

PREPARED STATEMENT OF KEN CORNICK, CO-FOUNDER AND PRESIDENT, CLEAR

Good Morning Chairman Sullivan, Ranking Member Markey and Members of the Senate Commerce Subcommittee on Security.

My name is Ken Cornick, I am a co-founder of CLEAR and the company's President. I am honored to be in front of you today.

Following the 9/11 attacks, Congress passed the Aviation and Transportation Security Act of 2001. This legislation led to the creation of the Registered Traveler or RT program. Congress' goal was to both enhance security and improve the traveler experience. In 2006, under the Federal registry notice, multiple RT providers began operations. Unfortunately, RT providers fell victim to the Great Recession and in 2008, ceased operations.

My partner and CLEAR's CEO Caryn Seidman Becker and I purchased CLEAR's assets in 2010. Soon after, we received approval from TSA to relaunch CLEAR and opened our first two airports in Orlando and Denver.

CLEAR has grown significantly since then, as travelers have recognized the efficiency of our biometric process and airports have recognized the security, customer service and economic benefits of adopting CLEAR. By year-end, CLEAR will have ~5 million members in 35 of our Nation's largest airports. CLEAR processes almost 5 percent of the Nation's originating air passengers daily using biometrics, and upward of 10 percent in the airports we operate in.

We have had a significant and positive economic impact in the communities in which we operate, as we have created over two thousand jobs and shared tens of millions of dollars with our airport partners.

CLEAR is a secure identity platform. As an American-owned company, our mission is to innovate to strengthen our Homeland's security and delight consumers with frictionless experiences.

Our secure enrollment platform establishes an impermeable link between one's identity and biometrics. Our process entails:

1. Digitally authenticating a traveler's government-issued identification.
2. Establishing that the person enrolling is the person on such document through the use of challenge questions driven by commercially available data.
3. Capturing biometric data including fingerprints, iris image and face.

The enrollment process takes approximately five minutes and can be completed at any CLEAR location. Once completed, the traveler can use CLEAR immediately anywhere in our network for identity verification.

Our success is driven by a strong public-private partnership with TSA. This partnership is a win-win for all stakeholders—driving innovation, enhancing security, and efficiency for travelers at zero cost to taxpayers. CLEAR is a force multiplier for TSA—bringing significant additional resources to the checkpoint.

We support TSA's efforts to drive checkpoint efficiency through the introduction of new technology at the checkpoint and have numerous ideas that would enable CLEAR to further collaborate with TSA in the areas of biometrics and identity. Further, CLEAR is eager (and has offered) to invest its own capital, technology, and labor at the checkpoint to support TSA in its mission.

We can and want to do more with TSA—we see many areas for collaboration, particularly as TSA pushes toward the use of biometrics at the checkpoint and beyond. We have vast experience and expertise in biometrics, credential authentication, biometrics deployment, identity management, and more.

As CLEAR has grown, we have always maintained the underlying Congressional intent of the Registered Traveler program—improving overall security and enhancing the customer experience. We have done this while driving innovation to the checkpoint.

Given the world we live in I think it is important to address data security, which is core to our business. We have invested significantly in cybersecurity to ensure our systems are best in class. CLEAR is subject to regular TSA audits and as a result of our investments and TSA's oversight, we have been designated FISMA-High by TSA—the highest government cyber compliance rating available.

CLEAR's platform is also SAFETY Act Certified by the Department of Homeland Security as a Qualified Anti-Terrorism Technology.

In addition to securing our operations and our customers' data, we take the privacy of our members very seriously. CLEAR is a 100 percent opt-in service and we do not sell customer data.

Customer service is another key element of CLEAR's culture. Our 2,200+ passionate team members, also known as Ambassadors, are all SIDA badged, trained on security as well as customer service. Our employees are widely recognized as Ambassadors for the entire airport.

They are always available to help any traveler, answer questions, be the extra eyes and ears or just be a friendly face at the screening area. We have also begun training our Ambassadors on human trafficking prevention.

As a result of our relentless focus on security and customer service, we have become an instrumental partner for several premiere travel companies including Delta Air Lines, United Airlines, Hertz, and American Express.

CLEAR's partnership with Delta Air Lines started in 2016 and continues today. Our partnership offers a discounted CLEAR membership for Delta frequent fliers and helped launch CLEAR into several new airports, including Atlanta, JFK, and other Delta hubs. Since then we have expanded our relationship with Delta to offer biometric lounge access and biometric boarding passes and are currently working with Delta on new and exciting innovations to improve the customer experience.

Our second airline partnership, with United Airlines, was announced this past July. This partnership is already off to a great start; already tens of thousands of new United customers have joined CLEAR and we will soon bring CLEAR to United terminals in Chicago, Houston and Newark. We are also working with United on new innovations that will improve the travel experience for their customers.

Overall, we are delivering on seamless and secure travel experiences from the curb to the gate. Specifically, we are working with our partners to permit quick entry into lounges, board an international departure with nothing more than your face and check your bag with your fingers.

As we open CLEAR lanes throughout the United States, our partnerships bring great benefits to travelers and the communities we serve. For example, when Delta partnered with CLEAR, we entered Atlanta, Detroit, Minneapolis and Salt Lake City, bringing dozens of new jobs to each of those communities. When CLEAR enters O'Hare, Newark and the United terminal at Houston Intercontinental, we will create 200 new jobs across those three cities. On average, our Ambassadors are paid more than \$20 per hour and receive amazing benefits to include generous parental leave, full healthcare benefits and opportunities for our Ambassadors to advance.

This year, we will share approximately \$40 million with our airport partners and their communities as part of our airport operating contracts.

Beyond the airport, we think about the travel ribbon and making travelers' journeys seamless and frictionless from the time they leave their home in the morning until they are in their hotel room that night in another city. We are committed to constantly innovating and improving the travel experience.

One example of this commitment is our partnership with Hertz. Today, we have 14 Hertz Fast Lanes Powered by CLEAR, where Hertz President Club members can drive off the lot with their face. This program started in late-2018 and will grow to encompass top Hertz locations throughout the United States.

CLEAR also has a partnership with Major League Baseball. Today, we have 24 sports partners including the Minnesota Twins, Texas Rangers, Miami Heat and Seattle Seahawks, and we recently launched our first collegiate partner—the University of Texas at Austin.

We are not stopping at just airport security or travel/entertainment. We have use cases that focus on improving the customer experience and reducing fraud in health care, biometric payment, age validation, and access. We have exciting announcements planned in those areas in the coming weeks.

I want to thank the Committee for its support of the Registered Traveler program and its efforts to strengthen the program to ensure that it remains an important part of our Nation's aviation security layered defense.

I will close by asking Congress to support a modernization of the RT program and the use of biometrics in aviation security. We have come a long way since 9/11, but we have much work to do. By working with Congress, TSA, our airport and airline partners, and other stakeholders. We know we can continue to support TSA's mission and the congressional goals of improving security and delighting travelers.

Senator SULLIVAN. Thank you, Mr. Cornick.
Ms. Nelson.

**STATEMENT OF SARA NELSON, INTERNATIONAL PRESIDENT,
ASSOCIATION OF FLIGHT ATTENDANTS-CWA, AFL-CIO**

Ms. NELSON. Chairman Sullivan, Ranking Member Markey, and members of the Committee, my name is Sara Nelson. I am the International President of the Association of Flight Attendants-CWA representing 50,000 flight attendants at 20 airlines. Thank you for the opportunity to testify today as a key stakeholder and partner in airport security.

Before continuing, I would like to pause to recognize with profound sadness the passing of the Honorable Elijah Cummings. His was a voice of great moral clarity. We will miss the wisdom and strength with which he fought for working people, for his beloved Marylanders, and for our Nation.

On September 11, 2001, I was a Boston-based flight attendant, and before 9/11 I worked United flight 175 frequently. It could have been me on that fateful day, but instead it was people I knew and worked with and loved, including my good friends: Amy King, Michael Tarrou, Amy Jarret, Kathryn Laborie, Robert Fangman, Al Marchand, Alicia Titus, Marianne MacFarlane, and Jesus Sanchez. Security is personal for me and my flying partners. It is also fundamental to our ability to do our job.

I remember airport security prior to September 11. I remember the faces of the screeners who allowed the terrorists entrance to terminal C at Logan and the ability to board flight 175. I remember the screeners' faces because they were there all the time, 7 days a week, all hours of the day. I remember the sounds of their voices, their tired smiles, and their efforts to work long hours for the lowest bidding security company just so they could provide for their own families. I lost my friends, my profession was changed forever, but I also often wonder about those security agents and how they have coped with their part in failing to stop the most fatal attack on U.S. soil. Do they understand they were set up to fail?

On a fairly regular basis, there has been an attempt to return to the old system where security checkpoints were contracted out to the lowest bidder. Any system that puts security second to profits borders on reckless and is unjustified regression from TSA's successful mission, quote, to protect the nation's transportation systems, to ensure freedom of movement for people and commerce.

We strongly support maintaining a professional Federal Transportation Security Administration workforce. Federalizing airport screening has been a success. Improving the security of air travel and providing a rigorous review of our aviation security with oversight by legislators and input from aviation stakeholders and the traveling public. Crew and passengers are safer today because of it.

We commend the efforts of TSA Administrator David Pekoske and the entire agency for extraordinary efforts during the 35-day government shutdown. Transportation security officers who were required to report for work faced stress of unpaid bills and uncertainty about when they would resume getting a paycheck. This is an enormous distraction for the people charged with handling security on the front lines. The shutdown stretched people and resources and it put our security at risk. It should never be repeated,

and resources allocated to airport security should never be diverted. We urge lawmakers to ensure funding is adequate and stable to maintain the successful mission with TSA.

Safety and security does not just happen. It happens because we all work together to make it happen. Every day when flight attendants report to work at America's airport before we step onto the plane and assume our role as aviation's first responders, we rely upon well trained transportation security officers to ensure our safety and security and that of the flying public.

Yet, this workforce of 44,000 Americans do not have the guarantees and benefits of the Fair Labor Standards Act or the general schedule pay scale and they do not have the representation rights accorded by Congress to most of the Federal workforce under the Civil Service Reform Act of 1978. TSOs cannot appeal adverse personnel decisions even though TSA managers, cargo inspectors, and TSA administrative personnel have those rights. These are rights I work to protect for flight attendants, and what we should expect for the transportation security workforce. Congress should act to accord TSOs these rights and ensure safer skies by passing Senate bill 944, the Strengthening American Transportation Security Act of 2019.

On Saturday afternoon, August 24, 2019, TSA announced changes to the Known Crew Member program, or KCM, without consulting unions representing airline crew members. This resulted in confusion and misunderstanding among crew members, as well as TSA personnel, as to what procedures were going to be implemented and when. It also raised concerns about purpose of the sudden change, causing distractions across aviation. In the future, anytime TSA considers changes to KCM or the standard security program for airlines or airports that affect crew members and flight security, the agency should interface with flight attendant and pilot unions to ensure the most successful implementation of programs and maintain confidence in our overall security.

I would like to again thank the Chairman, Ranking Member, and members of the Committee for this opportunity to testify. We are proud of our work as aviation's first responders and the last line of defense in aviation security. We appreciate your attention and diligent efforts to ensure we have the proper tools to perform our work and to keep U.S. aviation safe and secure.

[The prepared statement of Ms. Nelson follows:]

PREPARED STATEMENT OF SARA NELSON, INTERNATIONAL PRESIDENT,
ASSOCIATION OF FLIGHT ATTENDANTS-CWA, AFL-CIO

Chairman Wicker, Ranking Member Cantwell and Members of the Committee:

My name is Sara Nelson, International President of the Association of Flight Attendants-CWA, AFL-CIO (AFA), representing 50,000 Flight Attendants at 20 airlines. Thank you for the opportunity to testify today on improving airport security. This subject is critically important to aviation's first responders. We also serve as the last line of defense in aviation security.

TSA Workforce

Flight Attendants strongly support maintaining a professional, Federal Transportation Security Administration workforce as part of the overall solution to safety and security in commercial aviation.

On September 11, 2001, I was based in Boston as a United Airlines flight attendant. Before 9/11, I had worked United flight 175 frequently. It could have been me

on that fateful day, but instead it was people I knew and worked with, including my good friends Amy King, Michael Tarrou, Amy Jarret, Kathryn Laborie, Robert Fangman, Al Marchand, Alicia Titus, Marianne MacFarlane, and Jesus Sanchez. Security is very personal for me and my flying partners. It is also fundamental to our ability to do our jobs.

I remember airport security prior to September 11th. I remember the faces of the screeners who allowed terrorists entrance to terminal C at Logan and the ability to board flight 175. I remember the screener's faces because they were there all the time, 7 days a week, all hours of the day. I remember the sounds of their voices, their tired smiles, and their efforts to work the long hours for the lowest bidding security company just so they could provide for their own families. I lost my friends, my profession was redefined and our world changed forever, but I also often wonder how those security agents have coped with their part in failing to stop the most fatal attack on U.S. soil. Do they understand they were set up to fail?

When airport security was federalized, security improved immediately. When TSOs took over airport security, my personal security improved dramatically. When TSOs won the right to be represented by the American Federation of Government Employees (AFGE), our security improved again because TSOs finally had a voice in their workplace. Efforts by TSA to standardize training at the Federal Law Enforcement Training Center has also created a more cohesive program and unified commitment to TSA's mission.

AFA further supports full collective bargaining rights for Transportation Security Officers to negotiate for better working conditions, putting TSA officers on the General Schedule pay scale, and providing officers with much needed statutory worker protections such as the Rehabilitation Act against unfair labor practices. We believe these worker rights are integral to maintaining a strong, engaged workforce for aviation security.

Safety and security doesn't just happen; it happens because we all work together to make it happen. My colleagues and I depend on TSA workers to keep our jobs safe. Federalizing airport screening has been a success, improving the security of air travel and providing a rigorous review of our aviation security with oversight by legislators and input from aviation stakeholders and the traveling public. Crew and passengers are safer today because of it. We continue to depend upon a regulated security system that meets the requirements of *The Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Commission Act)*, Pub. L. 110-53.

Adequate Long-Term Funding

Effective passenger and baggage screening is a vital part of our layered defense against terrorism in the skies. It is also a difficult job with massive responsibility.

On a fairly regular basis there has been an attempt to return to the old system where security checkpoints were contracted out to the lowest bidder. To return to a bottom-line driven system that puts security second to profits borders on reckless and is an unjustified regression from TSA's successful mission 'to protect the Nation's transportation systems to ensure freedom of movement for people and commerce.'

The Flight Attendants of this country act as first responders every day of the year and our lives depend on the integrity of each layer of security in the airport and on the aircraft. TSA must have the consistent, long-term funding to give screeners the staffing, support and training they need to do their jobs to help keep our skies safe and secure.

Government shutdowns result in weakened aviation security. Transportation security officers who are required to report for work without getting paid during a shutdown face added stress over unpaid bills and uncertainty about when their paychecks will resume. This is an enormous distraction for the people charged with handling security on the frontlines.

We commend the efforts of TSA Administrator David Pekoske and the entire agency for extraordinary efforts during the 35-day government shutdown. Under extraordinarily difficult situations, the Administrator and the entire Federal workforce worked around the clock to maintain airport security and the ability for aviation to continue service. The shutdown stretched people and resources. It put our security at risk. It should never be repeated.

Before the deadline in September of this year, Congress passed a stopgap spending measure to fund the government through November 21, 2019. While this averted another Government Shutdown in September, we are once again setting up a cycle of short-term funding measures for aviation safety and security. This will further slow work on the implementation of the Act. The Senate Homeland Security Committee estimates that the 35-day Government Shutdown cost the DOT 2,413 years

in worker productivity¹. Further, the dedicated work of Federal employees deserves our respect and support with long-term funding measures.

We also oppose diverting funding and resources from TSA to other security initiatives, such as border security. Reduced staffing at checkpoints isn't just an inconvenience—when TSA is stretched thin, it increases the risk of a serious security breach.

Flight Attendants often bear the brunt of travelers frustrated by any inefficiencies in security screening, making our workspace more volatile. Long lines also threaten air travel ticket sales and on-time operations. Diverting resources, cuts to funding, or failure to lock in long term funding can delay purchase of advanced screening equipment and other mission-critical investments designed to keep travelers safe and improve the efficiency and effectiveness of security, as well as undermine programs to support TSA workers and keep them on the job.

We urge lawmakers to ensure funding is adequate and stable to maintain the successful mission of TSA.

Known Crewmember Program

Known Crew Member is a risk-based screening program that recognizes airline crew are subject to extensive background and criminal records checks to ensure security and safety of flight. In light of the trusted status of airline crew with FAA Certification, the Known Crew Member program provides alternate, expedited screening procedures. This helps to properly allocate more TSA resources to lesser known persons accessing the sterile areas of airports.

On Saturday afternoon, August 24, 2019, TSA announced changes to the KCM program without consulting unions representing airline crew members. This resulted in confusion and misunderstanding among crew members as well as TSA personnel as to what procedures were going to be implemented and when. It also raised concerns about purpose of the sudden change, causing distractions across aviation.

While we believe there are many lessons to be learned from the initial program change announcement from TSA, we also want to recognize the immediate response and problem-solving efforts of Administrator Pekoske and Deputy Administrator Cogswell. TSA worked closely with our union and the Air Line Pilots Association to receive our concerns and proposed solutions to maintain the integrity of the program with the most efficient procedure changes for crew and TSOs alike.

In the future, any time TSA considers changes to KCM or the standard security program for airlines or airports, that affect crew members and flight security, the agency should provide notice in advance to union security representatives in order to obtain union input and perspective on how to best achieve the goals that TSA has identified. Past experience has shown that such input is valuable and benefits aviation security operations. Crewmember unions and airlines are necessary industry stakeholders that should be regularly informed and engaged for the most successful security programs and operational implementation.

Current Legislation

AFA supports two pieces of legislation before this committee. The Faster Act (S. 472) which would ensure aviation security service fees pay for the costs of security screening and the Cyber AIR Act (S. 2181) which would help protect from and require disclosure of any attempt or successful cyber-attacks.

Conclusion

I would like to again thank the Chairman, the Ranking Member and the Members of this Subcommittee for this opportunity to testify. We are proud of our work as aviation's first responders and the last line of defense in aviation security. We appreciate your attention and diligent efforts to ensure we have the proper tools to perform our work and keep U.S. aviation safe and secure.

Senator SULLIVAN. Thank you, Ms. Nelson, for that compelling testimony, and all the witnesses for very informative opening statements.

I am just going to throw this out to literally everybody here at the witness table kind of on the big issue that we are focused on here in terms of an oversight hearing.

¹Shutdown cost DOT, DHS thousands of years in lost productivity, POLITICO Pro, <https://t.co/O3478qNmFc?amp=1>, September 17, 2019

So as I mentioned and Senator Markey mentioned, last year we passed the TSA Modernization Act. It contained the most comprehensive overhaul of TSA since the creation of the agency after 9/11. And some of the notable requirements that expand PreCheck enrollment options, create new checkpoint lane configurations, establish new vetting standards for airport security badges—we were trying to address proactively some of the security issues.

But what I would like to get from all of the witnesses here is, have these provisions from last year's bill affected airports and airlines negatively, positively? Is the TSA moving quickly enough to implement these new provisions, and is there coordination happening with the different stakeholders, which are all represented here in this hearing, to implement some of these areas? And what did we leave out? We thought that was a pretty good bill. I think a number of you did, but obviously we did not cover the whole area.

So if we can just start with that, and maybe, Mr. McLaughlin, if you can kick it off as an airport manager, and then I literally want to hear from all the witnesses on that overarching question and really the purpose of this hearing.

Mr. McLAUGHLIN. Thank you.

I would say that in essentially a year, there has definitely been steps in the right direction. I think some of those steps have not been materialized. So, for example, I will talk about CT for a quick second.

We have been selected as one of TSA's airports for the CT program. We will receive six units, two in each of our checkpoints. We are just now in the process where we have a site survey coming up where we will begin the planning to deploy those units across the airport.

Frankly speaking, that is not a lot of time in my opinion to get something new and complex like this rolled out. So I am not displeased with the timing. I share that just as an example to say many of the things that you all have put in motion have not been realized yet, but we are starting to see the beginning phases of that.

Senator SULLIVAN. Great.

Ms. Barnes, other witnesses? Do you want to address that overarching question?

Ms. BARNES. Sure. So we are very supportive of the work that you all have done and are grateful for the advancement of the legislation. From our review, many of the deadlines have not yet been met, and we would like to see faster implementation in particular on some of the biometric opportunities.

Senator SULLIVAN. And have you addressed that with TSA?

Ms. BARNES. We have an upcoming meeting next week.

Senator SULLIVAN. OK, good. Well, we would like to hear what their response is.

Ms. BARNES. Absolutely. I would be happy to report back.

Senator SULLIVAN. Others? Ms. Beyer?

Ms. BEYER. So again, as I said in my testimony, many of the provisions in the TSA Modernization Act were critical initiatives for the airlines. So to your question about has it impacted our work with TSA positively, the answer would be absolutely, sir.

We have had multiple discussions from the airlines' side with TSA on their progress toward implementing a number of the provisions. As I noted in my testimony—and I would agree with Mr. McLaughlin—there are many things included in that bill. So we understand the workload that that puts on the agency. However, we very much would like to see the remainder of those provisions that are outstanding fully implemented as quickly as possible.

But, again, some of our key focus areas are carrying a lot of the air cargo security work to fruition, particularly on identifying additional technological resources for the screening of air cargo and innovation as well.

Senator SULLIVAN. Mr. Cornick?

Mr. CORNICK. Thank you.

I think from an innovation perspective, we would like to do more with TSA. So pushing biometrics further on an opt-in basis into the checkpoint is a focus of ours.

Senator SULLIVAN. Do you think they are doing that at a rate that is acceptable, or is it taking too long in that area?

Mr. CORNICK. I do not have an opinion on if it is going fast enough. All I know is that we are reaching about 5 percent of the nation's volume using biometrics, and I think to get real ubiquity with biometrics is going to be a team effort. A public-private partnership is important because you have got a passport database with face. You have got fingerprints in the PreCheck enrollment data base. But I think ultimately if you really want to penetrate the domestic market and get ubiquity with biometrics, it needs to be a public-private partnership.

Senator SULLIVAN. Ms. Nelson?

Ms. NELSON. What we have experienced just like with the FAA is the interruption of resources and the strain on the workload as Ms. Beyer referenced with the government shutdown, with the short-term funding that does not provide for the ability to plan long-term, and also with the diversion of the resources. It is taxing and does not provide the resources to do what has been mandated by Congress.

So we also just want to note that that has also been very taxing on the TSA interfacing with stakeholders, and I am going to allocate some of those decisions that have taken place on their part to that. We can do a better job with interfacing with stakeholders, and the GAO report from this last week identified that as well.

Senator SULLIVAN. Thank you.

Senator Markey.

Senator MARKEY. Thank you, Mr. Chairman.

I want to come back to this question of the diversion of the security fee. For this Fiscal Year, it will be \$1.3 billion, which is being raised ostensibly to protect the security of the flying public, but yet that money is just going to go into deficit reduction for the Federal Government.

So I would just like to come down and ask each of you, do you believe that we should ensure that all of that funding goes actually toward what its goal is as we are putting a fee on passengers in our country? So, Ms. Barnes, do you think that money should not be diverted and just going to security?

Ms. BARNES. Yes, Senator, we agree with you that we should not divert the fees. They should be entirely used for security and are supportive of your bill to do so.

Senator MARKEY. Mr. McLaughlin?

Mr. McLAUGHLIN. Yes, sir. If you had told me 10 years ago that airports would be paying for security technology, I would have said that is crazy. And yet here we are today forced into that situation.

Senator MARKEY. Thank you. Just expand on that. I mean, there is funding.

Mr. McLAUGHLIN. Right. I should not have said forced into that situation. We are making a choice to buy the latest and greatest technology because of our growth, because of our passengers' need. But a decade ago, that would not have been the way it would have been thought of.

Senator MARKEY. Because?

Mr. McLAUGHLIN. TSA would have—

Senator MARKEY. Because TSA would have paid for it with the \$1.3 billion that is just going to be diverted this year and the \$20 billion since 2013 that has been diverted. So it actually is an additional cost that has to be borne.

Ms. Beyer?

Ms. BEYER. Yes, Senator. As I said before, we are fully supportive of your bill to end the diversion of the TSA passenger security fee. Our passengers continue to pay this fee and not receive the benefit for which it was intended. We think there is no better way to enhance aviation security in this country than to rededicate those resources where they belong.

Senator MARKEY. Thank you.

Mr. Cornick?

Mr. CORNICK. We agree entirely with you, and we think that the more resources that are dedicated to the airport security, the better off everybody is.

Senator MARKEY. Ms. Nelson?

Ms. NELSON. The FASTER Act should be passed right away. It is a disservice and dishonest to the American public to continue to allow a diversion of these fees.

Senator MARKEY. Thank you.

And, again, Mr. McLaughlin, you put your finger right on it. You wind up having to find other ways of funding that. And how do you fund it?

Mr. McLAUGHLIN. So for us, we are in a position where we are funding it internally.

Senator MARKEY. Who pays for it? Where do your revenues—

Mr. McLAUGHLIN. Ultimately our stakeholders and our passengers.

Senator MARKEY. So in other words, the passengers pay a fee that then goes to the Federal Government that then gets diverted to deficit reduction, and then you impose a fee on the very same people in order to raise the money in order to buy the technology that they had already paid for by the fee that had originally been imposed upon them in order to fly out of the Denver airport. Is that correct?

Mr. McLAUGHLIN. Yes. We cover our fees through rates and charges which ultimately are passed to passengers.

Senator MARKEY. So it winds up as double taxation——

Mr. McLAUGHLIN. Yes.

Senator MARKEY.—in order to get the level of safety which modern threats require you to implement.

So let me move over then to the Known Crew Member program. That is particularly valuable. The program allows TSA to verify the identity of trusted airline employees such as pilots and flight attendants and expedite their airport security screening, which both reduces the number of people in passenger screening lines and protects us from insider threats.

Ms. Nelson already made reference to this. The TSA made abrupt and disruptive changes to the Known Crew Member program without consulting or providing advance notice to the relevant stakeholders, including airline pilots and the flight attendants themselves who are the subject of the rule.

And that is why I sent a letter to the TSA this week urging the agency to work more closely with our crew members moving forward. Crew members are our eyes in the sky. As Ms. Nelson said, they are the last line of defense trying to detect something that might go wrong that would jeopardize the security of the passengers on those planes.

So, Ms. Nelson, has the TSA historically consulted your union and other stakeholders before making changes to Known Crew Member or similar programs, and do you believe that the TSA has sufficiently committed to working with you moving forward?

Ms. NELSON. In the past when there have been changes to the Known Crew Member program or implementation of new procedures, there has been quite a bit of consultation with our union and with other crew member unions. That has worked very well because we have been able to all be on the same page, airlines, TSA, and the crew unions, to be able to communicate these changes and have everyone understand what is going on.

Administrator Pekoske and Deputy Administrator Cogswell did absolutely respond to our concerns, and I want to commend them for——

Senator MARKEY. After the fact.

Ms. NELSON. After the fact. And I want to commend them for working very closely with us on our concerns and trying to resolve those issues. They continue to do that, but I do think it is important to continue to lift up the importance of working with stakeholders so that we can have a program that works for our security, that unburdens the TSA to be able to focus on the real threats in the airport, that allows the crews to have full confidence in our security because there is not confusion out there on the line.

Senator MARKEY. And I believe that going forward robust collaboration with the flight attendants and other stakeholders is absolutely essential to ensuring that any rules that we have in place actually are the most effective that they can be, and it should be informed by those who are on the front lines.

Ms. NELSON. They will be the most effective, and we will be the most efficient with our security.

Senator MARKEY. Thank you.

Thank you, Mr. Chairman.

Senator SULLIVAN. Well, I have a few more questions, and I am hoping that some of our colleagues are likely going to return because this is a very important topic.

But let me ask Ms. Beyer and Mr. McLaughlin. Air cargo is extremely important for our country. It is extremely important for my state. The Ted Stevens-Anchorage International Airport is the second largest U.S. airport for landed weight of cargo, aircraft, and fifth largest in the world for air cargo throughput.

The TSA Modernization Act, as you know, created a new office at TSA dedicated to air cargo. How has the creation of this air cargo office improved the security and efficiency of air cargo moving through U.S. airports, and what more should TSA be doing in collaboration with industry and others to implement this?

Ms. BEYER. Thank you, Mr. Chairman, for the question.

As you noted, the air cargo office within TSA has recently been established. So it is early days still, sir. They have made good progress but, for example, full staffing under the organization is still pending. So we are working with TSA as they get to full capacity for that office.

As I noted, there are a number of very important air cargo initiatives that we would like to see move forward. Key among them is flexibility in screening options. Unlike passenger screening checkpoints or checked baggage, air cargo screening is performed by the industry. But we need TSA's support to evaluate and perform research and development and certify programs and technologies so that very diverse, complex air cargo environments can be addressed and we have options to perform that screening.

Senator SULLIVAN. Mr. McLaughlin, do you have a view on the air cargo issue?

Mr. McLAUGHLIN. So as proud as we are of our airport, admittedly we are not the cargo super power that you all are.

Senator SULLIVAN. I am glad you acknowledged that.

[Laughter.]

Mr. McLAUGHLIN. But I will say I think the cargo is growing in Denver as well, and we see tremendous potential in the future. So what we are really looking for today—I will tell you that we are getting everything that we need.

But there is a future that is right on our horizon, and Senator Markey really pointed out well the fact for us to get the whole equation right. And that means the screening of that cargo has to be effective, but it also has to be very efficient. The model is changing in air cargo, and the screening model has to be able to keep pace with the transition of cargo through hubs like Denver.

Senator SULLIVAN. OK. Thank you.

Let me ask Mr. Cornick on the issue which I think is a very interesting one in terms of efficiency, but also security is on the use of biometrics that your company is very focused on, updated computer tomography machines and other screening technologies. A lot of that is in, as you talked about, the Registered Travel program.

How is TSA collaborating with external partners like your company to help both not only expand this, but also make sure that the security of our airline system continues as this expansion occurs?

Mr. CORNICK. Thank you for the question.

So there are a couple elements to that question.

First I would start with on the cyber side. TSA has been collaborating with us from a cyber perspective.

Senator SULLIVAN. What does that mean? What do you mean when you are talking about this?

Mr. CORNICK. Well, data security. At the end of the day, biometrics are really zeroes and ones. It is data and you have to encrypt that data. And TSA has put forth standards that we have met, and they have audited us to those standards. So we are designated a FISMA-High company from a cyber perspective, which is the highest Federal level of data security. So from that perspective, we have been collaborating on the data security to make sure our system is best in class.

TSA is rolling out something called credential authentication technology, which validates that a driver's license or a passport is actually real. The traveler would present data at the time of travel. CLEAR has been doing credential authentication technology since 2010. That is our core process. We enroll someone. We validate it is a REAL ID and we bind that identity to their biometrics. And that is closing the identity loop. That is really, really important. So we take CAT, credential authentication, one step further, and we are combining it with biometrics, so we call it BAT. And so that is a really important program.

The next step is to link it to Secure Flight. That is TSA's back end that houses all of the security data, whether you are a PreCheck flyer, standard, or you are a selectee. And that connectivity into CAT is something that as a FISMA-High company we think would be a great addition to the RT program to have that direct connectivity into Secure Flight. So if you are a registered traveler coming through the CLEAR lane, for example, we know who you are using biometrics and we can get real time data on your level of security. Are you PreCheck? Are you standard? That is the similar connectivity as other private entities like airlines, airports, and private companies that do screening on behalf of TSA.

Senator SULLIVAN. Thank you.

Senator Lee.

**STATEMENT OF HON. MIKE LEE,
U.S. SENATOR FROM UTAH**

Senator LEE. Thank you so much, Mr. Chairman.

Thanks to all of you for being here to answer questions on these important issues.

Mr. McLaughlin, I would like to start with you, if we could.

On May 7 of this year, the FAA released a document on UAS detection systems, talking about their use at airports. The FAA's statement noted as follows, "the FAA does not support the use of counter-UAS systems by any entities other than Federal departments with explicit statutory authority to use this technology, including requirements for extensive coordination with the FAA to ensure safety risks are mitigated."

In light of recent events, including those that occurred at Gatwick, I believe airport authorities are rightly concerned about safety and security threats that can be posed either by people who

are behaving with malicious intent or, alternatively, those who are simply behaving recklessly.

Currently how vulnerable do you believe airports are to the threats posed by either the malicious or the reckless use of drones?

Mr. McLAUGHLIN. Thank you for the question.

I think to start the answer it really is important to note—and this is often said in this industry—that if you have seen one airport, you have seen one airport. Each airport has its own sort of vulnerabilities and its own natural fortifications, if you will. So the answer may be different for all of us.

Speaking specifically for Denver, I would say that we have support systems in place that keep us relatively safe. Other airports, based on their configurations, may be in a different state. What we have seen in the last several months is real coordination between Federal, State, and local officials, including by the way us. So we participate in regional working groups on drones and how to deal with them and how to identify them, what to do once they are identified.

And it is important to note that not all drones are nefarious. As you pointed out, in some cases people may be using them recreationally in the wrong places. But I would also argue that I think there is a future where we can use drones productively in our environment as well.

So we want to make sure that FAA has a balanced approach, one, ensuring that we have opportunities to detect—and you have talked about some of the work that is going on there—two, that there are coordinated efforts to be able to handle an actual drone event, again using a coordinated approach, and then finally, a process in place that makes it relatively easy, simple but obviously still protected for us to use drones in a way that makes sense in the airport environment, whether that is perimeter security or other things.

Senator LEE. Thank you. That is helpful and consistent with what I have been thinking.

The FAA's guidance seems a little ambiguous, but it seems also to imply to me that counter-UAS systems used by anyone other than the Federal Government could be illegal. If this is the case, what other recourse does an airport sponsor have to deal with these kinds of threats? And do we need to clarify the law? Is some additional authority necessary in order to empower you to keep people safe?

Mr. McLAUGHLIN. It is an incredibly difficult question. And as I sit here, I think about spending most of my career charged with protecting aviation. And so there is a tricky balance. Right? So on the one hand, being dependent on a Federal agency all the time to take that final drastic action seems limiting. On the other hand, to not have really specific and strong safeguards in place seems dangerous as well.

So what I think is really important right now—and let us be honest. This is still a relatively new issue. There is an ongoing dialogue that I think is really productive, and I think that dialogue is going to produce really good results as long as every voice is heard and every stakeholder is at the table. So my hope would be that we continue to get to a place where there is a balanced out-

come with drones. One, how do we ensure that the good ones are being used for the right reasons? Two, how do we detect the bad ones? And three, what do we do with them once those bad ones are in a place that they are compromising our operation?

Senator LEE. By the way, were you able to consult with the TSA as the TSA drafted its tactical response plan?

Mr. McLAUGHLIN. Absolutely.

Senator LEE. And are you currently implementing the technical response plan?

Mr. McLAUGHLIN. So yes. I am sorry. I did not mean to cut you off.

Senator LEE. No. I was finished. At your airport.

Mr. McLAUGHLIN. Yes. So we are working very closely with them. And I will say again in our case even before that directive came out, a lot of really good work had been done. And I will tell you that while the directive gives TSA rights and authorities, they did not come in heavy-handed. Rather, they came in as a partner to help work with us on what we would do in the event that we needed to execute the plan.

Senator LEE. Well, I appreciate your comments, and I especially appreciate your acknowledgement. I had never heard it expressed that way. You have seen one airport. You have seen on airport. And it would be folly for us to assume as a government that what works in Denver necessarily works in San Francisco, San Diego, Salt Lake City, Washington, D.C., or anywhere else. And that is why I am hoping we can give you the discretion and the authority that you need and clarify any ambiguity to make sure that you can keep flyers safe. Thank you.

Senator SULLIVAN. In Alaska, we call that one size does not fit all from the Federal Government. And I think we see that daily in this town.

Senator LEE. Although most of our states could fit inside of Alaska easily.

[Laughter.]

Senator SULLIVAN. Well, we are just getting these great shout-outs to Alaska today. Thank you, Senator Lee.

Senator Markey.

Senator MARKEY. Thank you, Mr. Chairman.

Actually what we saw on 9/11 was that Mohamed Atta and the others were coming through Portland, Maine and penetrating the security there, and then when they reached Boston, there was already an assumption that they had been cleared. So just thinking about the interconnectivity of this entire defense system that we try to put in place is absolutely critical.

And I agree with Ms. Nelson that the personnel in Boston were traumatized because they could actually retrospectively see those people walking around Logan because they had been scoping out the airport for months before they did it, and they could actually in their mind's eyes still see those people sitting there, thinking that they had been cleared coming through before.

Let me move on to another question if I may, and that is the question of facial recognition because, as we work to keep pace with emerging security threats, an aviation traveler's civil liberties cannot be an afterthought. At airports across the country, both

TSA and Customs and Border Protection are increasingly using facial recognition technology and collecting sensitive biometric data about travelers. Yet, the public lacks enforceable rights and rules to protect travelers' privacy and addresses the unique threats that TSA's biometric data collection poses to our civil liberties.

So, Mr. McLaughlin, do you agree that any collection of Americans' biometric information at airports should always be voluntary?

Mr. McLAUGHLIN. Yes, I do.

Senator MARKEY. Do you agree that TSA should enact enforceable rules and take all necessary steps to secure that biometric data it collects is secure?

Mr. McLAUGHLIN. Yes.

Senator MARKEY. Do you agree that TSA should enact binding safeguards to ensure that its use of biometric technology does not disproportionately burden or misidentify people of color?

Mr. McLAUGHLIN. Absolutely, yes.

Senator MARKEY. I agree with you. I agree with all of your answers. We are, however, quickly moving toward a point of no return when it comes to the deployment of facial recognition technology. TSA should stop using these invasive tools in the absence of formal rules that reflect our values and protect our privacies. All of this should be out there as the set of security protections not just to make sure nothing bad happens in terms of security for these airlines, but also nothing happens to the security of the individuals who should also have their rights protected and they are ensured that their privacy is not being unnecessarily invaded.

So that is always the challenge for us in the government. The technologies themselves are inanimate. They are only as effective as the human values which we build into them. We have to decide. And here, we still do not have a formal set of rules that are on the books, especially to protect minorities and others who could, in fact, have their identity be compromised.

So I thank you, Mr. McLaughlin. And once again, I call upon the agency to formalize these rules. It is absolutely essential. We should not be moving forward until we have decided what those protections are going to be.

Let me move on next to something else that we know, and that is those who mean to do us harm could try to exploit any technological vulnerability in our aviation system. And that means we need to discuss issues beyond TSA oversight that are also critical to safety in our skies.

One top area of concern is the cybersecurity standards and practices of airlines and aircraft manufacturers. Our airplanes are increasingly computerized, and new software is being rolled out every single day. Evolving technologies offer enormous potential to improve safety and to entertain passengers. But it will only take one hacker to access an aircraft's navigation or flight control system to cause an unforgettable disaster.

Regrettably, after investigating the cybersecurity of our aviation system, I discovered that although airlines may frequently experience attempted cyber attacks, their protocols and protections for cyber incidents need much improvement.

I also found that industry collaboration on cybersecurity is inconsistent. And that is why I, again with Senator Blumenthal, have

reintroduced the Cyber Air Act. The Cyber Air Act would require the airline industry to share information about cybersecurity vulnerabilities and direct the FAA to establish cybersecurity protections for aircraft.

Ms. Nelson, I am glad that you expressed support for our legislation. Can you explain the importance of cybersecurity in the skies from a crew member's perspective as we see this enhancement of technology in the airlines of our country?

Ms. NELSON. Well, crew members literally put their lives on the line when they go to work, and they expect that all security measures are going to be adequately measured and in place and any mitigation factors in place as well. We know this issue very well because, as the FCC was considering adding mobile broadband to our aircraft, we consulted with security experts, tactical experts and discovered a range of scenarios that created many vulnerabilities related to cybersecurity. We shared those privately—that is not something I would share in this open forum—but ultimately were successful in getting an interagency working group to assess these issues.

This is another area where you talk about collaboration within the industry and reporting this and sharing information that is absolutely crucial to our security. And the Cyber Air Act will ensure that we continue to maintain the mandates of the 9/11 Commission report to continue to assess what the risks are today and what mitigation factors need to be in place. And we need full information and collaboration to be able to do that.

Senator MARKEY. Do you agree with that, Mr. McLaughlin?

Mr. McLAUGHLIN. I do. So obviously cybersecurity in the air is really not my domain. On the ground we are committed to cybersecurity. We have instituted a scalable framework based on NIST that allows us to ensure that our systems are intact and safe.

Senator MARKEY. One of the things that was very clear after 9/11 is that Mohamed Atta was a very highly educated individual and many others who came to Boston. The 10 of them who came to Boston on that day to hijack those two planes that ultimately flew into the World Trade Center—they were sophisticated people. But they were looking for the aperture. They were looking for the way in that would be easiest for them. And it turned out that they could do so just with box cutters. And because of the lack of security, thinking about that as a threat, the lack of imagination, we saw the catastrophe.

Here, we are faced with another situation where there are highly sophisticated individuals who would exploit a vulnerability, exploit a point, an aperture that might make it possible for them to create a disaster. And if we do not have in place the rules, the protections, the understanding, the collaboration with those who are on the front lines, we could just see a repetition although using a more modern way in order to attack, but finding the vulnerability.

That is what was true with cargo. If we are going to screen our bags as we are going through, make us take off our shoes, and yet let cargo from people who are not even on the plane then to go onto the same vessel, well, that is crazy. That is crazy. So they will find and exploit these kind of vulnerabilities.

So do any of the others of you want to speak about this need to deal with the cybersecurity issues on these planes? Ms. Beyer?

Ms. BEYER. Certainly, Senator.

So I agree with you that cybersecurity is an extremely important issue, and airlines take it very seriously, sir. When I talked earlier about safety and security of our passengers and our crew members, that includes cybersecurity, and we are very aware of those challenges.

Airlines are continuing to invest in our cybersecurity infrastructure, as well as in ensuring robust information exchange both at the government and other industry partners. We do this in a number of ways. Two I would mention today. The first is participation in the aviation ISAC is very critical for that—

Senator MARKEY. ISAC stands for?

Ms. BEYER. Oh, that is a test. Sorry. It is a cyber-related consortium of entities that is specifically set up to exchange real-time information about cyber risks and cyber incidents. And our airlines are active participants.

The second one that I wanted to mention, sir—and I can get back to you on the exact acronym. Apologies.

The second one that I wanted to mention, sir, is that we actively participate in regular stakeholder meetings with the Aviation Cyber Initiative. That is a U.S. Government interagency body, tri-chaired by the Department of Homeland Security, the FAA, and the Department of Defense. And we are actively engaged in those conversations with those agencies as well.

Senator SULLIVAN. One follow-up. I want to make sure asking Ms. Barnes a couple questions.

Senator MARKEY. If I may. Are you happy, Ms. Nelson, with the level of cooperation you are receiving in terms of this conversation about broadband or additional technologies being introduced without a proper understanding of the potential vulnerabilities?

Ms. NELSON. We believe the Cyber Air Act would close loopholes.

Senator MARKEY. Good. Thank you. Appreciate it.

Senator SULLIVAN. So a couple more questions. I want to make sure—Ms. Barnes had a couple questions directed at her from a very important industry. We just actually had a big tourism conference in Juneau, Alaska just last week, over 600 attendees. And so we certainly want to make sure we are protecting the traveling public, but we are also making sure that we can help increase this important industry in our country in terms of tourism.

So I have three questions for you.

Have you found that the TSA's transportation security officer staffing at security checkpoints is keeping pace with the growth in passenger traffic, tourism traffic?

Are there other solutions you think that need to be implemented or looked at by the Congress or TSA to handle the increase in passenger volume?

And in your opening statement, you did talk about the REAL ID requirements, and I think it is a concern. I know that two states will not even start issuing compliant licenses until June 2020. That is Oklahoma and Oregon. How well is TSA doing in informing the traveling public about that?

I am throwing a lot at you there, but I wanted to make sure you had the opportunity to go into some details on issues that I know impact the tourism industry.

Ms. BARNES. Well, thank you, Chairman, and thank you for your leadership on all travel-related issues and your work to elevate the industry at large within the government because that is a really important—

Senator SULLIVAN. We have a bill coming out soon that we worked closely with you on, and hopefully it will get bipartisan support in this committee.

Ms. BARNES. And we are very appreciative of that and thank you for your leadership.

I will take the last question first. With regard to REAL ID, we are working with TSA and DHS to help to make sure that the traveling public is aware of this upcoming ID requirement. But what we are really concerned by is that 57 percent of Americans do not even know that the deadline is coming.

Senator SULLIVAN. How can we address that? We, the Federal Government, writ large, State governments, others.

Ms. BARNES. Well, I think PSAs, talking to your constituents, making sure that folks are aware. The airports have been rolling out what the TSA has been providing.

But we have launched an education initiative within the entirety of the industry, including our airports and airline colleagues, with CLEAR and others because we think that—you know, we have as many as 99 million Americans that are not REAL ID-compliant. And so if 80,000 people show up perhaps on October 1, 2020 and are turned away, that is just not acceptable. And as you noted, Oregon and Oklahoma are not even issuing REAL ID-compliant licenses until next summer.

But you also have 50 different applications of getting a REAL ID, plus D.C., and the territories. You have got a state like Washington State that has a different symbol. It does not have a star. You have a state like Maryland who has been issuing noncompliant REAL ID licenses. So they are requiring folks to come back. You have a state like New Jersey that is actually only implementing REAL IDs or issuing REAL IDs in two locations in their state. So we have a really inconsistent application of the requirements. And that is really why this broader education effort is required.

But on top of that, we should be allowing enrollees in CLEAR and TSA PreCheck who have already given a stronger identification, their biometric, than is required to get a REAL ID license. So we think automatically allowing them to be considered REAL ID-compliant as soon as—that is one that Congress would need to articulate or direct TSA to move forward on. And we think that would be a huge help.

We also think moving to a mobile type of enrollment allowing DMVs to do mobile enrollment and use mobile licenses would help to accelerate the REAL ID process so that more folks have those.

And then we are also, from an education standpoint, recommending that for those that are not able to get a REAL ID license in states like Oklahoma and Oregon that they move forward and get a passport now or enroll in a CLEAR or TSA PreCheck application.

Senator SULLIVAN. Thank you.
 Senator Blumenthal.

**STATEMENT OF HON. RICHARD BLUMENTHAL,
 U.S. SENATOR FROM CONNECTICUT**

Senator BLUMENTHAL. Thanks, Mr. Chairman, and thank you for allowing me to come back. I was on the floor. I apologize for missing some of the hearing.

And I am glad that all of you are in favor of returning the security fee that passengers pay back to the TSA. Ms. Nelson provided a really moving and eloquent account of how all of us are affected, the people who work in the industry, as well as the traveling public, by the threat to our security. And I think that fee is tremendously important.

I want to focus on a different issue that was raised I think or has been raised by Ms. Nelson. I think you recently called for a ban on e-cigarettes from planes. Maybe you could expand on your concerns about the threats that these devices pose when they are carried on a plane.

Ms. NELSON. Thank you very much for that.

We have lithium ion batteries on the aircraft all the time. They are in all kinds of devices that people carry, and some people may be carrying as many as six on them at any time.

The number of times that we have had a runaway device or runaway battery that has created smoke or flames, potentially heading toward combustion on the plane has been much higher, a much higher rate with the e-cigarettes. And so for that reason, we believe it is very important that FAA look very closely at these particular devices. There is a history here. When Samsung had a device that was improperly flaming, there was a ban on those devices. So there is a history here. We think they need to look very closely at these e-cigarette devices which have had a higher instance of failing on board the aircraft and putting passengers and crew in danger.

Senator BLUMENTHAL. And I am troubled by some of the reports recently of weak enforcement of the checked baggage, and I am quoting from the "Washington Post" of October 7, just days ago. Quote: in March, Southwest Airlines employees had to pull a smoking suitcase containing e-cigarette batteries from a plane's cargo hold in San Diego. Adjacent bags were damaged, as was the plane, which was temporarily taken out of service.

So I am concerned that the DOT in May 2016, which banned these devices from checked baggage, may have really been insufficient to address—and I am quoting—the safety risks posed by the battery-powered portable electronic smoking devices. End quote. I welcome your view that consideration ought to be given to going further.

Let me ask Ms. Beyer what your organization thinks about this issue?

Ms. BEYER. Certainly, Senator. Thank you for the question.

Airlines care deeply about safety. And I am aware that FAA already has regulations for transport of lithium ion batteries. For us, anytime there is consideration of additional measures, whether they be safety- or security-related, we believe that that should be considered under the principles of risk-based security.

I think in this particular instance, Senator, what would be required is a very thoughtful process to determine whether technology in the checked baggage environment is currently capable or should be capable of screening for safety-related concerns rather than just security-related concerns such as explosives. So that is what we would advocate for, sir.

Senator BLUMENTHAL. Let me ask you finally. After 9/11, Congress mandated reinforced flight deck doors on commercial aircraft to add a valuable level of protection for the cockpits. But reinforced doors alone may not provide a complete solution to the problem that they were intended to resolve. There are times when operational necessity requires that the flight door be open while the plane is in flight.

The FAA Reauthorization Act of 2018, as you know, included an important security provision to address this issue. It required the FAA to mandate secondary cockpit barriers on all new passenger aircraft. Congress required the FAA to issue that rule by October 5, 2019. That day has come. It is past. Instead of meeting the statutory deadline, last month—or rather, on October 5, the FAA announced that the selection of secondary barriers—the working group intended to produce a recommendation on the rule.

You are a member or your organization is a member on that working group. Could you give us an update?

Ms. BEYER. Certainly, Senator.

So as you mentioned, A4A is a member on the working group under the Aviation Rulemaking Advisory Committee that was set up to look at and make recommendations to the FAA about implementing that mandate. We look forward to participating in that process and ensuring that all of the necessary information is collected and reviewed so that the provision can be implemented in such a way that it can actually be carried out and executed, things like considerations of the variation in aircraft fleet type, engineering considerations, training considerations, et cetera. All of those things are what we hope to bring to this working group for consideration.

Senator BLUMENTHAL. I think your organization said that, quote, secondary cockpit barriers were appropriate to certain types of aircraft. For what types of aircraft would they be inappropriate?

Ms. BEYER. So, sir, I am not aware of the exact quote that you are referring to, but I would certainly say Congress has weighed in on this particular issue on secondary barriers. And we will continue to collaborate with the FAA on the best way to implement that mandate.

Senator BLUMENTHAL. Well, maybe in response to a written question, you could be somewhat more specific.

My time has expired. I thank the Chairman for permitting me to ask these questions. Thank you.

Senator SULLIVAN. Absolutely, Senator Blumenthal.

We are going to wrap this hearing up, but I do want to take the opportunity very quickly, 30–45 seconds each of you, as the last element of this hearing just give us just a very quick summation of what you see in terms of the oversight issues are the most important that we should, as the members of this committee, remem-

ber and take away with us. So again, if you can do it in less than a minute, each of you, I would appreciate it.

Ms. Barnes, why do we not just start with you and go down the line?

Ms. BARNES. Sure. So thank you for the opportunity to be here today.

With regard to TSA, we think moving more quickly on the implementation of their work and moving more quickly in particular as they move the biometrics to the front of the TSA checkpoint.

Furthermore, there is a lot of work we need to do to make sure that America is REAL ID ready both via education and with the agency as well because, quite frankly, we cannot have a half a million flyers turned away at America's airports on October 1, 2020. And so we thank you for your help in ensuring that we are able to find policy solutions that can also help mitigate the negative consequences of this deadline.

Senator SULLIVAN. Great. Thank you and thank you for keeping that close to one minute.

Mr. McLaughlin?

Mr. McLAUGHLIN. Thank you again very much for the time here today.

For me it is a really simple message. Our industry is growing both in passenger traffic and in cargo. Current processes and current budgets will not keep up with that growth. We need your help in ensuring that we have the budgets to get where we need to go in the coming years. Thank you.

Senator SULLIVAN. Thank you.

Ms. Beyer?

Ms. BEYER. Certainly. Thank you.

I would agree with what Mr. McLaughlin said and also just to highlight again and underscore the importance both of stopping the diversion of the TSA passenger security fee. That money is critical for us as a government and industry to move this industry forward and ensure the security of our passengers and crew.

And also to underscore, again as Ms. Barnes did, the importance of educating the traveling public and avoiding a problem at our airports on October 1 of next year when the REAL ID enforcement deadline is set to be implemented.

Senator SULLIVAN. Thank you.

Mr. Cornick?

Mr. CORNICK. Thank you. Thank you for your continued support of the RT program. We ask that Congress continues to modernize the RT program and continue its support. We want to continue to be a force multiplier for aviation security and grow our public-private partnership.

Senator SULLIVAN. Excellent. Thank you.

And Ms. Nelson.

Ms. NELSON. Thank you very much.

Stable, secure funding with no diversion of that funding and passing of the FAST Act, continued and committed stakeholder involvement, including REAL ID. Flight attendants are on the front line and can help educate the public on this. And full representation rights for our TSOs.

And let me just also note that the Modernization Act was phenomenal. Thank you so much for your work on that. The one thing that we would say is missing from it is mandatory crew member self-defense training. We were the first to die, the last to be trained. And that goes right with our secondary cockpit barriers.

So thank you very much.

Senator SULLIVAN. Thank you. And I want to thank again all the witnesses today.

The hearing will remain open for two weeks. During this time, Senators may submit questions for the record. Upon receipt, the witnesses are respectfully requested to submit their written answers to the Committee as soon as possible but by no later than Thursday, October 31.

And I want to thank the witnesses again.

This hearing is now adjourned.

[Whereupon, at 12:05 p.m., the hearing was adjourned.]

A P P E N D I X

ELECTRONIC PRIVACY INFORMATION CENTER
Washington, DC, October 16, 2019

Hon. DAN SULLIVAN, Chairman,
Hon. EDWARD J. MARKEY, Ranking Member,
U.S. Senate Committee on Commerce, Science, and Transportation,
Subcommittee on Security,
Washington, DC.

Dear Chairman Sullivan and Ranking Member Markey:

We write to you in advance of the hearing on “Improving Security at America’s Airports: Stakeholder Perspectives.”¹ EPIC recently filed a lawsuit against the Customs and Border Protection (“CBP”) agency for a failure to establish necessary privacy safeguards for the use of facial images at U.S. borders.² Because the Transportation Security Administration (“TSA”) has failed to establish necessary privacy safeguards, including ensuring the travelers are able to exercise their legal right to opt-out, *we request you suspend the TSA’s use of facial image technology pending the completion of required public rulemaking by CBP.* A moratorium should also be established for other DHS components that propose to deploy facial recognition and have not conducted a public rulemaking. *There is currently no legal authority for DHS’ or TSA’s use of facial recognition technology.*

The Electronic Privacy Information Center (“EPIC”) is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues.³ EPIC is focused on protecting individual privacy rights, and we are particularly interested in the privacy problems associated with surveillance.⁴ We applaud Senator Markey and Senator Lee for calling for the suspension of DHS’s use of facial recognition in airports until a rulemaking to establish privacy and security safeguards is complete.⁵

Recently, new privacy risks have arisen with the deployment of facial recognition technology at U.S. airports following a 2017 Executive Order to “expedite the completion and implementation of biometric entry exit tracking system.”⁶ Customs and Border Protection (“CBP”) has now implemented the Biometric Entry-Exit program for international travelers at 17 airports.⁷ TSA is quickly moving to leverage CBP’s Biometric Entry-Exit program to expand the use of facial recognition at airports.⁸

TSA has conducted pilots at John F. Kennedy International Airport and Los Angeles International Airport to test facial recognition technology at security checkpoints servicing international travelers.⁹ TSA also tested a fully biometric terminal at Hartsfield-Jackson Atlanta International Airport that used facial recognition to

¹Improving Security at America’s Airports: Stakeholder Perspectives, Senate Comm. on Commerce, Science, & Trans., Subcomm. on Security, 116th Cong. (Oct. 17, 2019), <https://www.commerce.senate.gov/2019/10/improving-security-at-america-s-airports-stakeholder-perspectives/6e8bba82-9b59-4f09-b0c4-e8511497f5c4>.

²EPIC v. U.S. Customs and Border Protection, No. 19-cv-689 (D.D.C. filed Mar. 12, 2019); See <https://epic.org/foia/dhs/cbp/alt-screening-procedures/>.

³See About EPIC, EPIC.org, <https://epic.org/epic/about.html>.

⁴EPIC, EPIC Domestic Surveillance Project, <https://epic.org/privacy/surveillance/>.

⁵Press Release, Sens. Edward Markey and Mike Lee, *Senators Markey and Lee Call for Transparency on DHS Use of Facial Recognition Technology* (Mar. 12, 2019), <https://www.markey.senate.gov/news/press-releases/senators-markey-and-lee-call-for-transparency-on-dhs-use-of-facial-recognition-technology>.

⁶Exec. Order No. 13,780 § 8.

⁷Davey Alba, *The U.S. Government Will Be Scanning Your Face At 20 Top Airports, Documents Show* (Mar. 11, 2019), <https://www.buzzfeednews.com/article/daveyalba/these-documents-reveal-the-governments-detailed-plan-for>.

⁸TSA, *TSA Biometrics Roadmap* (Sept. 2018), https://www.tsa.gov/sites/default/files/tsa_biometrics_roadmap.pdf.

⁹TSA, *Facial Recognition Technology*, <https://www.tsa.gov/node/20451>.

check your bag, go through security, and board a flight,¹⁰ and is currently testing facial recognition at Las Vegas McCarran Airport.¹¹

The Las Vegas pilot is testing the “operational effectiveness for matching a traveler’s image to the photos on the ID they present.”¹² This 1:1 matching is a much more privacy protective implementation of facial recognition. 1:1 matching does not require a massive biometric database, there is no need to retain the image, and the machines conducting the 1:1 match do not need to be connected to the cloud. Such an implementation virtually eliminates data breach risks and the chance of mission creep.

But whether TSA is seriously considering a 1:1 implementation is not clear. The agency’s Aviation Security Advisory Committee has failed to fill the committee positions allotted for privacy advocates.¹³ And TSA’s on roadmap for facial recognition do not include the possibility for implementing 1:1 matching.

In September 2018, TSA released the “TSA Biometrics Roadmap.”¹⁴ The Roadmap makes clear TSA’s intention to leverage CBP’s facial recognition capabilities implemented as part of the Biometric Entry-Exit Program. But alternatives to CBP’s cloud-based implementation are not considered in the roadmap. And corresponding privacy safeguards have not yet been established despite TSA moving forward with facial recognition technology.

In response to an EPIC Freedom of Information Act request, CBP recently released 346 pages of documents detailing the agency’s scramble to implement the flawed Biometric Entry-Exit system, a system that employs facial recognition technology on travelers entering and exiting the country. The documents obtained by EPIC describe the administration’s plan to extend the faulty pilot program to major U.S. airports. The documents obtained by EPIC were covered in-depth by Buzzfeed.¹⁵

Based on the documents obtained, EPIC determined there are few limits on how airlines can use the facial recognition data collected at airports.¹⁶ Only recently has CBP changed course and indicated that the agency will require airlines to delete the photos they take for the Biometric Entry-Exit program.¹⁷ No such commitment has been made by TSA. Indeed, TSA’s Roadmap indicates that the agency wants to expand the dissemination of biometric data as much as possible, stating:

TSA will pursue a system architecture that promotes data sharing to maximize biometric adoption throughout the passenger base and across the aviation security touchpoints of the passenger experience.¹⁸

TSA seeks to broadly implement facial recognition through “public-private partnerships” to create a “biometrically-enabled curb-to-gate passenger experience.”¹⁹ TSA plans to implement an opt-in model of facial recognition use for domestic travelers but there are no guarantees that in the future TSA will not require passengers to participate in facial recognition or make the alternative so cumbersome as to essentially require passengers to opt-in.

Preserving the ability of U.S. citizens to forgo facial recognition for alternative processes is one of the core privacy issues with CBP’s Biometric Entry-Exit program.

EPIC recently sued CBP for all records related to the creation and modification of alternative screening procedures for the Biometric Entry-Exit program.²⁰ The alternative screening procedure for U.S. travelers that opt-out of facial recognition should be a manual check of the traveler’s identification documents. CBP, however,

¹⁰TSA, *TSA Releases Roadmap For Expanding Biometrics Technology* (Oct. 15, 2018), <https://www.tsa.gov/news/releases/2018/10/15/tsa-releases-roadmap-expanding-biometrics-technology>.

¹¹*Protecting the Nation’s Transportation Systems: Oversight of the Transportation Security Administration*, 114th Cong. (2019), S. Comm. on Commerce, Science, and Trans. (testimony of Patricia F. S. Cogswell TSA Acting Deputy Administrator), available at <https://www.tsa.gov/news/testimony/2019/09/11/protecting-nations-transportation-systems-oversight-transportation>.

¹²*Id.*

¹³TSA, *TSA Announces New Members of Aviation Security Advisory Committee*, (Sept. 27, 2019), <https://www.tsa.gov/news/releases/2019/09/27/tsa-announces-new-members-aviation-security-advisory-committee>.

¹⁴TSA *Biometrics Roadmap*, *supra* note 8.

¹⁵Alba, *supra* note 7.

¹⁶See CBP Memorandum of Understanding Regarding Biometric Pilot Project, <https://epic.org/foia/dhs/cbp/biometric-entry-exit/MOU-Biometric-Pilot-Project.pdf>.

¹⁷Ashley Ortiz, CBP Program and Management Analyst, Presentation before the Data Privacy & Integrity Advisory Committee, slide 23 (Dec. 2018), <https://www.dhs.gov/sites/default/files/publications/SLIDES-DPIAC-Public%20Meeting%2012%2010-2018.pdf>.

¹⁸TSA, *TSA Biometrics Roadmap*, 17 (Sept. 2018).

¹⁹*Id.* at 19.

²⁰*EPIC v. CBP*, 19-cv-00689, *Complaint*, <https://epic.org/foia/cbp/alternative-screening-procedures/1-Complaint.pdf>.

has provided vague and inconsistent descriptions of alternative screening procedures in both its “Biometric Exit Frequently Asked Questions (FAQ)” webpage²¹ and the agency’s privacy impact assessments.²² The creation and modification of CBP’s alternative screening procedures underscores CBP’s unchecked ability to modify alternative screening procedures while travelers remain in the dark about how to protect their biometric data.

Given the close relationship between the TSA’s implementation of facial recognition and CBP’s Biometric Entry-Exit program, *the Subcommittee should place a moratorium on TSA’s implementation of facial recognition until CBP implements proper privacy assessments, policies and procedures, and oversight mechanisms.*

Facial recognition poses threats to privacy and civil liberties. Facial recognition techniques can be deployed covertly, remotely, and on a mass scale. There is a lack of well-defined Federal regulations controlling the collection, use, dissemination, and retention of biometric identifiers. Ubiquitous identification by government agencies eliminates the individual’s ability to control the disclosure of their identities, creates new opportunities for tracking and monitoring, and poses a specific risk to the First Amendment rights of free association and free expression.

Before there is any increased deployment of these programs, CBP must conduct a public rulemaking and TSA must conduct a privacy impact assessment. And deployment of surveillance technology should be accompanied by new policies and procedures and independent oversight to protect citizens’ rights.

The use of facial recognition at the border has real consequences for U.S. citizens and non-U.S. citizens. All people entering the U.S., including U.S. passport holders, could be subject to this intrusive screening technique. The privacy assessments, policies and procedures, and oversight mechanisms must all be made public. Most critically, if the TSA creates or expand a system of records that contains personal information retrievable by name, it must comply with the requirements of the Privacy Act so that the public can comment on a record system established by a Federal agency.²³

We ask that our statement be entered into the hearing record.

Sincerely,

/s/ MARC ROTENBERG
Marc Rotenberg
EPIC President

/s/ CAITRIONA FITZGERALD
Caitriona Fitzgerald
EPIC Policy Director

/s/ JERAMIE SCOTT
Jeramie Scott
EPIC Senior Counsel

PREPARED STATEMENT OF AMERICAN FEDERATION OF GOVERNMENT EMPLOYEES,
AFL-CIO

Chairmen Wicker and Sullivan and Ranking Members Cantwell and Markey:

On behalf of the American Federation of Government Employees, AFL-CIO, which represents more than 700,000 Federal and District of Columbia employees who serve the American people in 70 different agencies, including the 44,000 Transportation Security Officers who protect the flying public, we appreciate the opportunity to submit this letter for the record on “Improving Security at America’s Airports: Stakeholder Perspectives.”

Transportation Security Officers (TSOs) are sworn to protect the Nation’s aviation security. They conduct themselves with the utmost professionalism and respect for the importance of the work they do. Every day, they identify and eradicate threats to aviation security. TSOs take pride in making sure all systems are working and that personnel are fully trained in operations and observing standard operating procedures to ensure security.

²¹ CBP, *Biometric Exit Frequently Asked Questions (FAQs)*, <https://www.cbp.gov/travel/biometrics/biometric-exit-faqs>.

²² U.S. Dep’t of Homeland Sec., DHS/CBP/PIA–030(b), *Privacy Impact Assessment Update for the Traveler Verification Service (TVS): Partner Process 8* (2017), <https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp030-tvs-may2017.pdf>; see also U.S. Dep’t of Homeland Sec., DHS/CBP/PIA–030(c), *Privacy Impact Assessment Update for the Traveler Verification Service (TVS): Partner Process 5–6* (2017), <https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp030-tvs-appendix-july2018.pdf>; U.S. Dep’t of Homeland Sec., DHS/CBP/PIA–056, *Privacy Impact Assessment for the Traveler Verification Service 2* (2018), https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp030-tvs-november2018_2.pdf.

²³ 5 U.S.C.A. § 552a(e)(4).

Today, we commend the Committee for its examination of airport security from the perspective of those whose work brings them to America's airports. They are the flight attendants who ensure in-flight safety, the air traffic controllers who secure every take-off and landing. When they come to work, their lives and livelihoods depend on the Transportation Security Administration (TSA) getting security right.

As the Committee considers the implementation of the TSA Modernization Act of 2018, we point out one provision of that Act, Section 1907, which required the TSA Administrator to convene a working group consisting of representatives of the TSA and representatives of AFGE to recommend reforms to TSA's personnel management system. Security screening requires a substantial investment in technology, but it is essentially a human function and thereby requires a commensurate investment in the personnel who carry out these crucial functions.

TSA's personnel management system is perhaps the worst in the Federal Government. It is a system that gives agency management tremendous discretion and very little accountability because it deprives employees of full due process and collective bargaining rights guaranteed to other Federal employees under Title 5. Under Title 5, personnel management is governed by a set of checks and balances that ensures merit system principles are upheld for the benefit of good government. Title 5 processes provide mechanisms that prevent managers from hiring, firing, demoting, or disciplining employees for bad reasons such as politics, bias, bigotry, or to shift blame for mismanagement. Because TSA's workforce has fewer and weaker protections against the consequences of mismanagement, it is unsurprising that the agency experiences massive turnover, low morale, and a low level of trust in management's decisions.

The recent decision to change the terms of coverage under the Federal Employees Health Benefits Program (FEHBP) for TSA's large "part-time" workforce is a good example of the misuse of authority in the area of personnel management. Without notice, bargaining, or rationale; without any mention during any of the Section 1907 Working Group meetings, TSA issued a "management directive" on September 20, 2019 that effected a reduction in the agency's contribution to FEHBP premiums for its part-time workforce. TSA defined part-time as all employees "assigned to work schedules of 32 hours or less per week (64 hours or less per pay period). . . ." Prior to the issuance of this directive, TSA paid the same portion of FEHBP premiums for its full-time and part-time workforce. Now, for those hired after September 30, 2019, FEHBP premiums will be pro-rated for those assigned to part-time schedules. Of course, the assignment of a part-time vs. a full-time schedule is at the sole discretion of management. Likewise, regular assignment of overtime for a "part-time" Transportation Security Officer (TSO) at management's discretion will not affect his or her status as a part-time employee with a lower employer subsidy for FEHBP.

When TSA was established and granted authority to have a large portion of its workforce on permanent part-time status in order to maximize its flexibility, it agreed to provide FEHBP coverage on the same basis for its part-time and full-time workforce. This arrangement was far from optimal, as the vast majority of those assigned to part-time schedules wanted and needed a full-time paycheck. The full FEHBP subsidy has served as an important offset to the undesirable and inadequate part-time schedule and associated salary. Indeed, TSA has acknowledged that low TSO salaries and involuntary part-time schedules have been large factors in creating the agency's difficulties with turnover and low morale, both of which undermine its ability to carry out its mission. Indeed, apart from the base meanness of the action, it is difficult to understand why TSA has decided to worsen its problems by cutting health insurance benefits for such a large portion of its workforce.

The decision to convene a Working Group under Section 1907 of the TSA Modernization Act of 2018 was a second-best effort to address TSA's deficient record on the use of its vast flexibilities and discretion in the area of personnel management. AFGE has argued strenuously that TSA's personnel management shortcomings will not be solved unless and until its employees are provided the same rights under Title 5 as other Federal employees, including Federal law enforcement officers elsewhere in the Department of Homeland Security. The Working Group was not a substitute for collective bargaining rights, which at TSA exist almost entirely at the whim of each subsequent Administrator. Thus the extent of these rights is highly politicized and varies with an administration's level of support toward the right of employees who elect union representation to engage in collective bargaining. Nevertheless, AFGE participated fully and in good faith in the Section 1907 Working Group meetings. As the surprise FEHBP reduction for a substantial portion of the TSO workforce shows, it is not at all clear that TSA participated on the same terms.

The Section 1907 Working Group met over several months this year and recently submitted its report to Congress. What was remarkable about the Working Group was that all proposals were made by the Group's AFGE members. Rather than a

robust discussion of the needs of personnel from both a management and labor perspective, the Agency's participation was primarily delivered in the form of decisions to recommend AFGE's proposals or decline them with little or no discussion. Included were proposals to change pay scales to incorporate regular and reasonable increases over time, essential decisions about fitness for duty, fair representation of the workforce including reasonable grievance procedures and neutral arbitration, and basic rights at work. Without fair pay and representation for its TSOs, TSA will continue to experience high turnover, requiring significant investment in rehiring and retraining.

Because TSOs are so essential to the security of the flying public, they should be under the same law that governs personnel management in the rest of the Federal Government. It is just as important to TSA's mission that its workforce have fair compensation, full due process and union rights as it is to every other component of DHS. During the historic 2018–2019 government shutdown, the Nation learned about the dedication and mettle of TSOs at the same time they learned of their meager pay and substandard rights on the job. Please remember that TSOs showed up at work every day during that difficult period. Many faced significant challenges to make ends meet as the shutdown dragged through three pay periods, but they kept their promise to the American public. TSOs are frequently required to perform mandatory overtime, are faced with ever-changing shifts and insufficient rest time between shifts, and management failure to execute the rotation of duties in accordance with standard operating procedures. These represent potential security risks, many of which we tried to address through the Working Group. Congress must understand that while AFGE did its best, TSA did not reciprocate and thus the Section 1907 of the TSA Modernization Act was not fully utilized to improve personnel management in a way that will enhance aviation security.

As the Committee continues to examine airport security, please know the workforce stands ready and determined to ensure the security of the flying public. TSOs take pride in their work protecting America's airports and skies. AFGE thanks the Committee for holding this important hearing and we look forward to working with you to address the aforementioned issues.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. TODD YOUNG TO
TORI EMERSON BARNES

Ms. Barnes, in your testimony you outline the four policy recommendations offered by U.S. Travel. The fourth recommendation is related to the implementation of biometric identity verification technology at TSA checkpoints.

Question. Can you speak to the critical need for TSA to utilize advanced technology to update their security strategy and elaborate on how TSA and DHS can effectively accelerate the implementation of biometric technology?

Answer. The development and deployment of various technologies have the opportunity to modernize the travel security process by both enhancing security and increasing traveler facilitation.

TSA released its Biometric Roadmap in October 2018. This report outlines how TSA plans to pursue and deploy biometrics technology at airports. The report has four stated goals: (1) Partner with CBP on Biometrics for international travelers, (2) Operationalize Biometrics for TSA PreCheck, (3) Expand Biometrics to additional domestic travelers, and (4) Develop infrastructure to support biometric solutions. We believe these are lofty, but necessary goals to move transportation security to meet modern traveler expectations and set the foundation for the future of secure travel.

In our view, the timetable for providing biometric identification options at travel checkpoints could significantly shorten if (1) DHS provided greater clarity on matters of public interest, (2) CBP and TSA capitalized on interagency synergy, and (3) both agencies gained access to more resources dedicated to this specific use-case.

First, public trust acceptance, and utilization will drive DHS forward. In an increasingly digital age, travelers are rightly concerned about data security and privacy. DHS should provide clarity about the application, collection, deletion, and sharing of all data within the travel security ecosystem. Specific standards will provide confidence to the travelling public that the technology is safe and secure. Similarly, DHS should provide data on the accuracy of the technology across locations and demographics, and set minimum standards for application. Providing the traveling public clarity on the security and accuracy of the technology will supplement the added facilitation benefits of operationalizing biometric technology. Integrating biometrics for Trusted Traveler enrollees, who have opted-in and been vetted, will provide significant facilitation benefits by expediting the traveler identification process that precludes the physical security system at airports.

Second, we believe significant gains could be made if TSA and CBP capitalized on each other's development and implementation process, taking advantage of any technology advancement, procurement opportunity, or insight gained throughout the process. To sustain momentum throughout the development cycle, both agencies should focus on the ultimate goal of embracing new technology and new capabilities to ensure long-term applicability, and not get bogged down on compatibility challenges tied to antiquated forms of identification. The ultimate goal should be to produce an identification system that is wholly independent from, and un-reliant on, card-based identification.

Third, TSA, CBP, and DHS will need resources to standardize, operationalize, and then expedite implementation. Investments in infrastructure, training, testing, and accuracy will be required to bring biometrics to the checkpoint, all of which will require significant new resources. Both TSA and CBP have a portion of their collected fees diverted to non-security related accounts and activities. Returning these fees to the accounts for which they were originally intended will have a significant benefit on the operations of both CBP and TSA. Additionally, dedicated appropriations will be needed to successfully expand the roll out of biometric identification beyond the test phase.

The travel industry applauded TSA for releasing their biometrics roadmap in 2018. We share the vision for utilizing technology for the screening of passengers because it has the potential to provide both faster and more secure travel. Now we must do the hard work of putting that vision into action. Congress and the Administration should work together to take the steps listed above and bring forward the day when Americans can have a safer, faster, and more convenient way to travel.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. DAN SULLIVAN TO
KEN CORNICK

Question 1. Mr. Cornick, how does TSA's current Credential Authentication Technology deployment plan impact your operations as a participant in the Registered Traveler Program?

Answer. TSA has publicly stated that when its Credential Authentication Technology (CAT) is deployed, all passengers including biometrically verified Registered Traveler (RT) participants will be required to be processed by the TSA Travel Document Checker (TDC) to be run through CAT. We believe this undermines the RT program and will cause passengers to question why they are taking the extra step to submit biometrics only to stop again at the TDC. Additionally, this eliminates any checkpoint efficiency gains that the RT program provides for TSA and the traveling public.

This challenge could be avoided with RT programs having transactional access to real time vetting status databases maintained by TSA. The technology to fulfill this request is available and could be implemented at no direct cost to taxpayers.

RT programs are force multipliers at the checkpoint providing additional resources with enhanced security, technology, innovation, and staff all at no cost to TSA.

Question 2. As a member of the Registered Traveler Program, would CLEAR agree to sign a Secure Flight access agreement with TSA that commits your company to ensuring privacy protection, data security, and any other necessary safeguards?

Answer. Yes. CLEAR has stated to TSA on any number of occasions its willingness to abide by any reasonable standards and requirements TSA may put in place as a precondition to gaining connectivity to SecureFlight. As an example, CLEAR has already invested a significant amount of time and resources for its technology platform to be certified by TSA as "FISMA High." This was done specifically in anticipation of gaining the aforementioned access. CLEAR welcomes the opportunity to collaborate with TSA on a SecureFlight access agreement.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. AMY KLOBUCHAR TO
CHRIS McLAUGHLIN

Earlier this month (in October 2019), I sent a letter to Administrator Pekoske urging the Transportation Security Administration (TSA) to increase the authorized staffing levels at Minneapolis-St. Paul International Airport (MSP) to help reduce increasing passenger wait times. While historically only 55 percent of passengers began or ended their flight at MSP, now 64 percent of passengers do, creating a significant increase in demand for screening services. In addition to increasing staff

levels, programs like TSA PreCheck can help speed up the security screening process.

Question. How do programs like TSA PreCheck help improve passenger wait times and the security screening process?

Answer. Senator Klobuchar, thank you for the important question and for your continued leadership on aviation security. While at TSA, I played a leadership role in the development and deployment of TSA's PreCheck program.

It is critical that TSA continue to advance its risk-based security initiatives. To date, TSA PreCheck has succeeded in its goal of enhancing security and improving the screening process for individuals enrolled in the program. However, the low overall enrollment rate has prevented TSA from achieving its ultimate goal of improving security and processing time for all passengers. As I stated in my testimony, TSA must continue to advance the PreCheck program and the best way to do this is through the third-party initiatives that Congress specified in the TSA Modernization Act.

I would like to take a deeper dive into the program to further answer your question.

At the macro level, TSA PreCheck improves both passenger wait times as well as the security screening process.

In terms of wait times, it's simple math; by leaving jackets, belts, and shoes on, and liquids and laptops in the bag, passengers process through physical screening more quickly than those that are subjected to traditional divestiture requirements. As a result, the larger we can grow the population of TSA PreCheck customers relative to "standard" customers, the faster the overall screening "system" will perform. Given the same number of TSA lanes and staffing, all passengers should wait less than they otherwise would have as the TSA PreCheck population grows.

It is interesting to note that many incorrectly believe that their individual line wait experience should be reduced with TSA PreCheck.

This wasn't the originally stated objective of the program, but rather a by-product of a fledgling program with an inadequate marketing engine to support it. Early TSA PreCheck adopters enjoyed empty lines and have since begun to expect them. The program developers had an expectation from the outset that the queues would eventually fill.

More importantly than wait times, TSA PreCheck improves overall security by utilizing an intelligence driven, risk-based approach. Individuals who volunteer identifiable information about themselves, and who therefore become more "known," present less of a security risk than individuals who are wholly unknown. Because TSA has limited resources, it makes sense from a security perspective to focus on individuals who are lesser known. Finding a non-criminal prohibited item being carried by a person with an unknown history of intent is a higher priority than finding the same item being carried by a person with no history of intent. No system is perfect, and "known" individuals aren't free of risk. Nonetheless, as a former TSA Administrator used to say, "TSA is in the business of risk mitigation, not total risk elimination".

Thank you for the question and please do not hesitate to reach out should you or staff want to discuss further.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. AMY KLOBUCHAR TO
LAUREN BEYER

Aviation safety is a priority for me, and I have introduced legislation with Senators Cantwell, Blumenthal, Markey, and Duckworth—the Safe Skies Act—to ensure that America's cargo plane pilots have the same rest requirements as passenger pilots.

Question. Can you speak to the importance of having strong rest requirements for both passenger and cargo pilots?

Answer. Aviation safety is ingrained in the culture of the U.S. aviation industry, and at the forefront of every aspect of all commercial operations, regardless of whether it is a passenger or cargo operation.

When addressing crew alertness and fatigue-related issues, it is important to understand the significant differences between cargo and passenger operations and ensure that the safety regulatory framework is capable of addressing the unique issues inherent in these operations. Congress did just that in 2010, in mandating that all air carriers, including cargo air carriers, have an FAA-approved Fatigue Risk Management Plan (FRMP). The FAA-approved FRMPs ensure that all air carriers have fatigue reporting programs, systems for monitoring pilot fatigue, processes for developing fatigue mitigation measures where needed, and training for crewmembers on

the risks associated with fatigue and steps they can and should take to mitigate these risks. As a result of this framework, carriers, including cargo carriers, have developed fatigue monitoring tools, invested in extensive fatigue mitigation measures, and continue to develop robust systems for monitoring pilot fatigue in order to adjust operations as needed. One set of prescriptive rules that applies to all will not serve to address the unique safety issues of the various types of operations we see today. The FAA and the industry stakeholders have acknowledged this and remain committed to developing fatigue science and collecting the necessary data to further advance fatigue risk management systems.

As a result of this framework, both passenger and cargo carriers strictly adhere to their respective FAA regulations and work proactively with their pilots to continually improve alertness and fatigue-related safety policies through their respective FAA-approved FRMPs that are reviewed regularly by the FAA.

We share your commitment to safety and would be more than happy to brief you and/or your staff on the significant efforts that take place every day to address alertness and fatigue-related issues for pilots. U.S. passenger and cargo carriers have a shared commitment to safety and have spent decades establishing the global standard for safety and security. We will continue to lead.

