INSIDER THREATS TO AVIATION SECURITY: AIRLINE AND AIRPORT PERSPECTIVES

HEARING

BEFORE THE

SUBCOMMITTEE ON TRANSPORTATION AND PROTECTIVE SECURITY

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

SEPTEMBER 27, 2018

Serial No. 115–77

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
34–448 PDF WASHINGTON : 2019

COMMITTEE ON HOMELAND SECURITY

MICHAEL T. MCCAUL, Texas, *Chairman*

LAMAR SMITH, Texas
PETER T. KING, New York
MIKE ROGERS, Alabama
LOU BARLETTA, Pennsylvania
SCOTT PERRY, Pennsylvania
JOHN KATKO, New York
WILL HURD, Texas
MARTHA MCSALLY, Arizona
JOHN RATCLIFFE, Texas
DANIEL M. DONOVAN, JR., New York
MIKE GALLAGHER, Wisconsin
CLAY HIGGINS, Louisiana
THOMAS A. GARRETT, JR., Virginia
BRIAN K. FITZPATRICK, Pennsylvania
RON ESTES, Kansas
DON BACON, Nebraska
DEBBIE LESKO, Arizona

BENNIE G. THOMPSON, Mississippi
SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
CEDRIC L. RICHMOND, Louisiana
WILLIAM R. KEATING, Massachusetts
DONALD M. PAYNE, JR., New Jersey
FILEMON VELA, Texas
BONNIE WATSON COLEMAN, New Jersey
KATHLEEN M. RICE, New York
J. LUIS CORREA, California
VAL BUTLER DEMINGS, Florida
NANETTE DIAZ BARRAGÁN, California

BRENDAN P. SHIELDS, *Staff Director*
HOPE GOINS, *Minority Staff Director*

SUBCOMMITTEE ON TRANSPORTATION AND PROTECTIVE SECURITY

JOHN KATKO, New York, *Chairman*

MIKE ROGERS, Alabama
BRIAN K. FITZPATRICK, Pennsylvania
RON ESTES, Kansas
DEBBIE LESKO, Arizona
MICHAEL T. MCCAUL, Texas *(ex officio)*

BONNIE WATSON COLEMAN, New Jersey
WILLIAM R. KEATING, Massachusetts
DONALD M. PAYNE, JR., New Jersey
BENNIE G. THOMPSON, Mississippi *(ex officio)*

KYLE D. KLEIN, *Subcommittee Staff Director*

CONTENTS

INSIDER THREATS TO AVIATION SECURITY: AIRLINE AND AIRPORT PERSPECTIVES

Wednesday, September 27, 2018

U.S. HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON TRANSPORTATION
AND PROTECTIVE SECURITY,
COMMITTEE ON HOMELAND SECURITY,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:04 a.m., in room HVC–210, Capitol Visitor Center, Hon. John Katko (Chairman of the subcommittee) presiding.

Present: Representatives Katko, Estes, Lesko, and Watson Coleman.

Mr. KATKO. The Committee on Homeland Security, Subcommittee on Transportation and Protective Security, will come to order. The subcommittee is meeting today to examine the risk insider threats pose to America's aviation system. I now recognize myself for an opening statement.

First, I want to acknowledge House passage of a comprehensive 5-year FAA reauthorization. This legislation also includes a full authorization of the Transportation Security Administration. This is the first time TSA has been reauthorized since the agency was stood up following the terror attacks of September 11.

This bipartisan bill includes not only 22 House-passed transportation security bills, but also a number of key provisions from last year's DHS authorization legislation.

I look forward to seeing this legislation move quickly through the Senate and to the President's desk so that we can implement unprecedented transparency and accountability at TSA and make the agency more adaptive to evolving threats to the traveling public.

Now, on to the topic of today's hearing.

When considering threats facing America's aviation sector, it is critical that we consider the security threats emanating from inside the sector itself. Insider threats can manifest themselves in a variety of ways, including drug and weapon smuggling, human trafficking, terror plots, and others.

For example, in 2013, Terry Loewen, an avionics technician at Wichita Mid-Continent Airport, was arrested by the FBI for plotting a suicide attack using a vehicle-borne improvised explosive device. Loewen intended to use his airport credentials to gain access to the tarmac and detonate the truck near aircraft and the passenger terminal during peak holiday travel to maximize casualties.

In 2014, Eugene Harvey, a baggage handler at Hartsfield-Jackson International Airport, smuggled 153 firearms, including AK–47

assault weapons, on 17 flights between Atlanta and New York. Harvey was able to bring the guns into the sterile area of the airport using a secure identification display area, or SIDA badge, because he was not subjected to physical security screening.

Additionally, in May 2018, 10 airline employees at Dallas/Fort Worth International Airport were indicted as part of an FBI undercover operation. The employees believed they were smuggling methamphetamines. One of the employees who was indicted said he would be able to smuggle guns as well, and another told undercover agents he would be willing to smuggle explosives for the right price. That is truly frightening.

Most recently, in August 2018, Richard Russell, a ground service agent at Seattle-Tacoma International Airport who held valid security credentials, entered an aircraft maintenance area and stole a commercial aircraft before crashing it to take his own life.

Just last week, a student pilot jumped a security fence at Orlando Melbourne international Airport and boarded a passenger jet that was undergoing maintenance. While it is unclear what his intentions were, there remain access control concerns surrounding that incident and many others.

This string of disturbing incidents clearly demonstrates the risk insider threats pose to our Nation's aviation system. I am concerned that the same vulnerabilities that were exploited in these situations could also be exploited by terrorists to carry out an attack.

Over the past few years, progress has certainly been made to address these gaps, especially with respect to pre-employment vetting and screening of aviation workers before entering the secure area of the airport.

However, the fact that these insider threats continue to manifest would seem to indicate that the current system has not proven to be a sufficient deterrent for employees with malicious intent.

This committee has passed multiple pieces of legislation dealing with aviation employee vetting and access controls, including my bill, H.R. 876, the Aviation Employee Screening and Security Enhancement Act of 2017, which should be headed to the President's desk as part of the FAA reauthorization.

While this bill has many provisions that will help mitigate insider threats, this is not an issue that can be dealt with solely through legislation. You all know it takes a lot more for me to acknowledge that.

At this hearing, the subcommittee has the opportunity to hear from a number of aviation stakeholders with varying perspectives on how we can respond to insider threats. The groups these individuals represent are on the front lines and have unique insight into how best to combat the threats facing our Nation's aviation system.

I look forward to discussing how we can better screen and vet aviation employees and improve access controls to help ensure the sensitive areas of our Nation's airports are secure.

I also look forward to hearing the witnesses' opinions on how the Federal Government can better work with industry to address any existing vulnerabilities in our current system.

I truly believe that close collaboration between all the relevant stakeholders—we are not interested in "gotcha" moments here today, we are just interested in a frank discussion—will be key to tackling the array of insider threats facing America's aviation sector.

I would like to thank all of you for showing up today, and I look forward to hearing your testimony.

[The statement of Chairman Katko follows:]

STATEMENT OF CHAIRMAN JOHN KATKO

SEPTEMBER 27, 2018

First, I want to acknowledge House passage of a comprehensive, 5-year FAA Reauthorization. This legislation also includes a full reauthorization of the Transportation Security Administration. This is the first time TSA has been reauthorized since the agency was stood up following the terror attacks of September 11.

This bipartisan bill includes not only 22 House-passed transportation security bills, but also a number of key provisions from last year's DHS Authorization legislation.

I look forward to seeing this legislation move quickly through the Senate and to the President's desk, so that we can implement unprecedented transparency and accountability at TSA and make the agency more adaptive to evolving threats to the traveling public. Now, on to the topic of today's hearing.

When considering threats facing America's aviation sector, it is critical that we consider the security threats emanating from inside the sector itself.

Insider threats can manifest themselves in a variety of ways, including drug and weapons smuggling, human trafficking, terror plots, and others.

For example, in December 2013, Terry Loewen—an avionics technician at Wichita Mid-Continent Airport—was arrested by the FBI for plotting a suicide attack using a vehicle-borne improvised explosives device.

Loewen intended to use his airport credentials to gain access to the tarmac and detonate the truck near aircraft and the passenger terminal during peak holiday travel to maximize casualties.

In 2014, Eugene Harvey, a baggage handler at Hartsfield-Jackson International Airport, smuggled 153 firearms, including AK–47 assault weapons, on 17 flights between Atlanta and New York.

Harvey was able to bring the guns into the sterile area of the airport using his Secure Identification Display Area—or SIDA—badge, because he was not subjected to physical security screening.

Additionally, in May 2018, 10 airline employees at Dallas/Fort Worth International Airport were indicted as part of an FBI undercover operation. The employees believed they were smuggling methamphetamines.

One of the employees who was indicted indicated he would be able to smuggle guns as well, and another told undercover agents he would be willing to smuggling explosives for the right price.

Most recently, in August 2018, Richard Russell, a ground services agent at Seattle-Tacoma International Airport who held valid security credentials, entered an aircraft maintenance area and stole a commercial aircraft before crashing it order to take his own life.

Just last week, a student pilot jumped a security fence at Orlando Melbourne International Airport and boarded a passenger jet that was undergoing maintenance. While it is unclear what his intentions were, there remain access controls concerns surrounding that incident.

This string of disturbing incidents clearly demonstrates the risk insider threats pose to our Nation's aviation system. I am concerned that the same vulnerabilities that were exploited in these situations could also be exploited by terrorists to carry out an attack.

Over the past few years, progress has certainly been made to address the gaps, especially with respect to pre-employment vetting and screening aviation workers before entering the secure area of the airport.

However, the fact that these insider threats continue to manifest would seem to indicate that the current system has not proven to be a sufficient deterrent for employees with malicious intent.

This committee has passed multiple pieces of legislation dealing with aviation employee vetting and access controls including my bill, H.R. 876, The Aviation Em-

ployee Screening and Security Enhancement Act of 2017, which should be headed to the President's desk as part of the FAA reauthorization.

While this bill has many provisions that will help mitigate insider threats, this is not an issue that can be dealt with solely through legislation—and you all know it takes a lot for me to acknowledge that.

At this hearing, the subcommittee has the opportunity to hear from a number of aviation stakeholders, with varying perspectives on how we can respond to insider threats.

The groups these individuals represent are on the front lines and have unique insight into how to best combat the threats facing our Nation's aviation system.

I look forward to discussing how we can better screen and vet aviation employees and improve access controls to help ensure the sensitive areas of our Nation's airports are secure.

I also look forward to hearing the witness' opinions on how the Federal Government can better work with industry to address any existing vulnerabilities in our current system. I truly believe that close collaboration between all the relevant stakeholders will be key in truly tackling the array of insider threats facing America's aviation sector.

I'd like to thank the witnesses again for being here today and I look forward to hearing their testimony.

Mr. KATKO. I am pleased to recognize the Ranking Member of the subcommittee, the gentlelady and good friend from New Jersey, Mrs. Watson Coleman for her opening statement.

Mrs. WATSON COLEMAN. Good morning and thank you, Chairman. Thank you for holding this hearing.

Thank you to the witnesses for being willing to share your experience, your concern, and your expectations of future things that we can do.

I also want to thank the Chairman for his collaboration in putting together the package of TSA legislation that he referred to and that was included in the FAA Reauthorization Act that passed the House yesterday.

By my count, the package included 21 TSA bills that originated in this subcommittee, reflecting the extent of our bipartisan work in this Congress and to the extent to which we have been listening to those who have come before us.

In addition to bills I authored to enhance surface transportation security and authorize TSA's National Deployment Force, the package includes several provisions relevant to today's hearing.

Congressman Keating's bill, the Airport Perimeter and Access Control Security Act, requires the TSA administrator to update key risk assessments and strategies guiding perimeter security and access control efforts.

Chairman Katko's bill, the Aviation Employee Screening and Security Enhancement Act, of which I am a co-sponsor, directs a cost and a feasibility study of enhanced employee inspections at airport access points as well as an assessment of credential standards.

These bills build upon provisions enacted in the 2016 FAA Extension Act that required TSA to update rules on airport access controls and improve criminal background checks.

TSA and industry stakeholders have worked to implement these requirements and other measures to enhance security, including recommendations made by the Aviation Security Advisory Committee.

For example, the TSA has developed the Advanced Threat Location Allocation Strategy, or ATLAS, to ensure limited resources for employee screening are deployed based on risk and in a manner

that maximizes the expectation among employees that they will be subjected to screening.

Airports and airlines, for their part, have worked hard to reduce access points to secure areas and improve security awareness among employees.

All parties deserve recognition for taking these threats seriously and coming to the table to develop sensible and effective solutions.

Nevertheless, recent incidents have made clear that significant vulnerabilities remain. Last month, the Horizon Air employee was able to steal and fly a passenger jet at Seattle-Tacoma International Airport, ultimately crashing it in what was fortunately an unpopulated area killing only himself. If this individual had different intentions or if we had simply been less lucky, the incident could have placed all of downtown Seattle in grave danger.

Then just a week ago, a student pilot was able to jump over a perimeter security fence at Orlando Melbourne International Airport and access a cockpit of a large passenger jet. Fortunately, two courageous maintenance workers were on board the plane and heroically disrupted the apparent plot to steal the plane.

Again, under slightly different circumstances, events could have played out much more negatively.

While the student pilot in Orlando was not an insider in the same way as an airline worker in Seattle, the incident highlighted the need to control access to aircraft more strictly, as well as the need to better secure airport perimeters.

It has also highlighted that these workers should not be viewed primarily as a threat to aviation, but rather as important security partners. Aviation workers know airports better than anyone. They know who should be where, and they recognize when something is out of place. Security solutions must be developed in consultation with workers and take full advantage of their expertise, as well as perhaps additional training on awareness standards.

Both of these recent incidents are being investigated, and I certainly am eager to learn more about the motives of the individuals in question and how they were able to defeat security measures so easily.

In the mean time, I hope our witnesses today will be able to shed some light on how similar incidences can be prevented in the future and what this committee can do to be helpful.

Thank you. I look forward to discussing the issues today. I yield back my time.

[The statement of Ranking Member Watson Coleman follows:]

STATEMENT OF RANKING MEMBER BONNIE WATSON COLEMAN

SEPTEMBER 27, 2018

I want to thank Chairman Katko for his collaboration in putting together the package of TSA legislation that was included in the FAA Reauthorization Act that passed the House yesterday.

By my count, the package includes 21 TSA bills that originated in this subcommittee, reflecting the extent of our bipartisan work this Congress.

In addition to bills I authored to enhance surface transportation security and authorize TSA's National Deployment Force, the package includes several provisions relevant to today's hearing.

Congressman Keating's bill, the Airport Perimeter and Access Control Security Act, requires the TSA administrator to update key risk assessments and strategies guiding perimeter security and access control efforts.

Chairman Katko's bill, the Aviation Employee Screening and Security Enhancement Act, of which I am a co-sponsor, directs a cost and feasibility study of enhanced employee inspections at airport access points, as well as an assessment of credentialing standards.

These bills build upon provisions enacted in the 2016 FAA Extension Act that required TSA to update rules on airport access controls and improve criminal background checks.

TSA and industry stakeholders have worked to implement those requirements and other measures to enhance security, including recommendations made by the Aviation Security Advisory Committee.

For example, TSA has developed the Advanced Threat Location Allocation Strategy, or "ATLAS," to ensure limited resources for employee screening are deployed based on risk and in a manner that maximizes the expectation among employees that they will be subject to screening.

Airports and airlines, for their part, have worked to reduce access points to secure areas and improve security awareness among employees.

All parties deserve recognition for taking these threats seriously and coming to the table to develop sensible and effective solutions.

Nevertheless, recent incidents have made clear that significant vulnerabilities remain.

Last month, a Horizon Air employee was able to steal and fly a passenger jet at Seattle-Tacoma International Airport, ultimately crashing it in what was fortunately an unpopulated area, killing only himself.

If this individual had had different intentions, or if we had simply been less lucky, the incident could have placed all of downtown Seattle in grave danger.

Just a week ago, a student pilot was able to jump over a perimeter security fence at Orlando-Melbourne International Airport and access the cockpit of a large passenger jet.

Fortunately, two courageous maintenance workers were on board the plane and heroically disrupted the apparent plot to steal another plane.

Again, under slightly different circumstances, events could have played out much more negatively.

While the student pilot in Orlando was not an "insider" in the same way as the airline worker in Seattle, the incident highlighted the need to control access to aircraft more strictly—as well as the need to better secure airport perimeters.

It also highlighted that workers should not be viewed primarily as a threat to aviation, but rather as important security partners.

Aviation workers know airports better than anyone. They know who should be where, and they recognize when something is out of place.

Security solutions must be developed in consultation with workers and take full advantage of their expertise.

Both of these recent incidents are being investigated, and I am eager to learn more about the motives of the individuals in question and how they were able to defeat security measures so easily.

In the mean time, I hope our witnesses today will be able to shed some light on how similar incidents can be prevented in the future and what this committee can do to be helpful.

Mr. KATKO. Thank you, Mrs. Watson Coleman.

It is really amazing that 21 of our bills that came out of this committee got into the FAA bill. It is really a great sign of the teamwork that we have on this subcommittee and the bipartisanship, because National security should not be a partisan issue, and it is certainly not in this subcommittee.

So I want to thank Mrs. Watson Coleman for her statement. Other Members of the subcommittee are reminded that opening statements may be submitted for the record.

[The statement of Ranking Member Thompson follows:]

STATEMENT OF RANKING MEMBER BENNIE G. THOMPSON

SEPTEMBER 27, 2018

Good morning and thank you to the Chairman for convening today's hearing.

Today's hearing is timely given recent events.

Twice in the last 2 months, unauthorized individuals have accessed cockpits of passenger jets.

In the first case, a ground crew worker at Seattle-Tacoma International Airport was able to commandeer an unoccupied plane, take off from the airport, and fly around the Seattle-Tacoma area for an hour before crashing in a wooded area, killing only himself.

In the second case, a student pilot with unclear intentions was able to hop a fence at Orlando-Melbourne International Airport and gain entry to an airplane cockpit before being tackled and detained by two workers who happened to be on the plane.

While the details of these events are still being investigated, it is clear that a major loss of life was prevented by sheer luck—and by the heroism of the two workers who acted bravely and selflessly to prevent catastrophe.

These events are the latest in a string of incidents displaying the challenges the aviation industry faces in controlling access to secure areas and aircrafts.

Each incident is unique and highlights slightly different vulnerabilities depending on the people and airport involved.

Given the complexity of the aviation system, no single solution will serve as a "silver bullet" to ensure sufficient security.

Instead, the TSA, airports, airlines, and other stakeholders must work collaboratively to develop and implement layered security measures that address security gaps and reduce risk as much as possible.

The Airport Perimeter and Access Control Security Act, introduced by Congressman Keating, will go a long way in directing that work by requiring TSA to update its risk assessments and strategies for perimeter security and access controls.

I was happy to see that bill included in the FAA Reauthorization Act that passed the House yesterday, along with 8 other Democratic bills and numerous other provisions that will strengthen TSA's security efforts across all modes of transportation.

Today, I hope to gain additional perspective on recent security incidents and learn from our witnesses what this committee can do to further support their security efforts.

I look forward to engaging in a productive discussion on these issues.

Again, thank you to the Chairman for his attention to these issues and to our witnesses for appearing before us today.

Mr. KATKO. We are grateful to have a very distinguished panel here to testify before us today. Let me remind each of you that your entire written statement will appear in the record.

Our first witness, Ms. Wendy Reiter, currently serves as the director of aviation security for Seattle-Tacoma International Airport. In this position, she leads the Port of Seattle's Aviation Security Department and oversees all TSA mandates that involve the safety and security of the 16,000 employees and travelers at the Sea-Tac Airport.

She joined the Port of Seattle as the senior manager of airport terminal operations in 2001, where she served as the primary liaison to airlines.

Prior to joining the Port of Seattle, Ms. Reiter was a station manager for Southwest Airlines—and you have got to get him to Syracuse, OK, I keep begging them—and director of customer service for Northwest Airlines, where she received numerous awards for leadership and outstanding customer service.

Before I recognize Ms. Reiter for her opening statement, I want to reiterate what I said during my opening statement. That is, we are not interested in gotcha moments here today. We are interested in a free-flowing, frank discussion about how we can make airports safer from an insider threat perspective.

So we welcome your input. Don't wait for us to call on you. If you have something, signal to us, and we will be happy to include you in the conversation.

So with that, I will recognize Ms. Reiter for her opening statement.

STATEMENT OF WENDY REITER, DIRECTOR, AVIATION SECURITY, PORT OF SEATTLE

Ms. REITER. Chairman Katko, Ranking Member Watson Coleman, and Members of the committee, thank you for the opportunity to join you again today. My name is Wendy Reiter, and I serve as the director of aviation security for Seattle-Tacoma International Airport.

Sea-Tac Airport has long prioritized the safety and security of our passengers, employees, and nearby residents. This commitment has driven Sea-Tac to do everything reasonable to invest in aviation security above and beyond what is required of us by Federal law, which has made us one of the leading airports in the country as it relates to insider threat and perimeter security.

I am pleased to be here today to share some of the specific tactics we have employed at Sea-Tac, although I will note that I am not here to suggest that all airports should adopt these exact practices. Sea-Tac recognizes that it is up to each airport's local leadership to determine how to best invest limited resources for maximum return.

Let me start with our approach to insider threat. First, before giving airport badges to employees and throughout the badge holder's employment, we work closely with the TSA and FBI to conduct regular background checks, both scheduled and unscheduled.

These badges allow us to restrict sterile areas to vetted employees and use access controls to limit specific areas of the airport and airfield to only the most relevant employees.

We are also planning, by end of this year, to be enrolled in the Rap Back program to ensure that badge access is immediately revoked from anyone with a newly-discovered disqualifying crime.

Second, each of our sterile area access doors requires both a bag scan and a biometric fingerprint scan. The biometric element has been in place at Sea-Tac since shortly after September 11, 2001, and it is an additional layer of security that allows us to confirm that the badge matches the users. In certain cases, we have added a third level of security to require a pin that is specific to the person.

Third, as of spring 2017, we have implemented physical screening to all employees accessing sterile areas of the airport terminal. Full employee screening required a significant upfront investment and major recurring cost to the airport, but we have been very pleased with results in terms of both security and employee convenience.

As it relates to perimeter security, our plan is to institute physical employee screening at all of our airfield perimeter gates by the middle of 2019.

We have also invested in three Air Scent dogs, which are trained to detect and trail explosive odors on moving persons, which is a huge advantage in the front of the airport around ticketing and baggage claim.

At the end of the day, all security systems are based on thoughtful risk management and no security system is perfect or able to anticipate every potential action. For instance, Sea-Tac experienced a high-profile insider incident just last month.

That is why Sea-Tac recently joined in creating a new Industry Working Group on Aviation Security Best Practices. The group will baseline aviation security best practices and our findings will be included in the final report of the TSA's ASAC Insider Threat Subcommittee, of which I am a member.

Specific topics for investigation include aircraft security, employee training and reward programs, mental health programs, and airport coordination operation centers.

Sea-Tac has also initiated an independent third-party after-action report of our most recent insider incident to identify other changes that our airport will consider.

I want to close by noting a series of activities coming together at the end of the year.

TSA Administrator Pekoske expects ASAC to report back to him, and the Sea-Tac after-action report and the industry working group findings will also be completed by that time.

Combined with the potential TSA and FBI reports on the recent Sea-Tac incident, the aviation community will have an incredible opportunity in early 2019 to thoughtfully discuss opportunities to move forward in impactful ways on insider threat.

I look forward to working with this committee and others at that time.

Thank you for your time today. I welcome any questions you may have.

[The prepared statement of Ms. Reiter follows:]

PREPARED STATEMENT OF WENDY REITER

SEPTEMBER 27, 2018

Chairman Katko, Ranking Member Watson Coleman, and Members of the committee, thank you for the opportunity to discuss aviation insider threat and perimeter security issues with you today. My name is Wendy Reiter, and I currently serve as the director of aviation security for Seattle-Tacoma International Airport (Sea-Tac), which is owned and operated by the Port of Seattle. I also recently served as vice-chair of the Transportation Security Services committee of the American Association of Airport Executives.

Sea-Tac Airport has long prioritized the safety and security of our passengers, employees, and nearby residents as our top responsibility. As an independent port authority governed by directly-elected Commissioners, protecting against threats both external and internal is a core part of our DNA. This commitment has driven Sea-Tac to do everything reasonable to invest in infrastructure, technology, and procedures that increase aviation security—above and beyond what is required of us by Federal law—which has made us one of the leading airports in the country as it relates to insider threat and perimeter security.

We deeply appreciate the partnership we have with the Transportation Security Administration (TSA), including both local TSA staff as well as TSA leadership in Washington, DC. I also want to thank the subcommittee for your work on the Checkpoint Optimization and Efficiency Act, which has resulted in improved collaboration, communication, and information sharing at the local level.

I am pleased to be here today to share some of the specific tactics we have employed at Sea-Tac, although I will note that we are not here to suggest that all airports should adopt these exact practices. As the old saying goes, "if you've seen one airport, you've seen one airport," and so we recognize that it is up to each airport's local leadership to determine how to best invest limited resources for maximum return. This is particularly true for insider threat issues, which may not be fully preventable no matter how many layers of security and redundancies are put into place.

Let me start with our approach to insider threat, which is mainly focused around three key aspects: Credentialing, biometrics, and physical employee screening. First, in terms of credentialing, we work closely with the Transportation Security Administration (TSA) and Federal Bureau of Investigation (FBI) to conduct regular back-

ground checks on all employees, both scheduled and unscheduled. Those badges not only allow us to ensure that sterile areas are restricted to vetted employees but also to use access controls to further limit specific areas of the airport and airfield to only the most relevant employees. We are also planning by the end of this year to be enrolled in the"Rap Back" program to ensure that badge access is immediately revoked from anyone with a newly-discovered disqualifying crime.

Second, each of our sterile-area access doors requires both a badge scan and a biometric fingerprint scan. The biometric element has been in place at Sea-Tac since shortly after September 11, 2001, and is an additional layer of security that allows us to confirm that the badge matches the user. In certain cases, we have added a third level of authentication to require the user to scan and swipe their badge as well as enter a uniquely assigned personal identification number (PIN).

Third, as of spring 2017, we have implemented physical screening for all employees accessing the sterile areas of the airport terminals. We have multiple checkpoints, each with a magnetometer, that are staffed by Port of Seattle employees hired specifically for this purpose. Full employee screening required a significant upfront investment and major recurring costs to the airport, but we have been very pleased with the results in terms of both security and employee convenience. We've been able to process as many as 300 employees per hour, and have now screened approximately 1.5 million individuals over the last year-and-a-half. This screening has resulted several times in the seizure of both weapons and drugs, which we believe we would have been not caught without such a system in place.

At Sea-Tac, we have 500 different employers operating at the airport, and there are limitations to the requirements that we can impose on all of those different entities and their workers. We rely on a partnership ethic to make any substantive changes to protocols and practices, and we are grateful for their openness to pursuing these important investments.

As it relates to perimeter security, Sea-Tac has made major investments in both employee screening and explosive detection canines. While we've had physical screening of employees inside the airport for the last year-and-a-half, our plan is to institute the same level of security at all of our airfield perimeter gates by the middle of 2019. This new procedure will require every person entering the airfield to walk through a magnetometer, and will include visual screening of all vehicles—again by specifically trained Port of Seattle staff.

We have also invested in purchasing our own explosive detection canines. In addition to the 8 Port of Seattle Police Department canine teams trained at the TSA canine training center at Lackland Air Force Base to sniff stationary objects for explosives, the Port 2 years ago purchased 3 Air Scent-trained dogs from K2 Solutions in North Carolina. These dogs are trained to detect and trail explosive odors on a moving person, which is a huge advantage in the front of the airport around ticketing and baggage claim. The Port Police are the first law enforcement agency in Washington State to have certified working Air Scent Teams.

At the end of the day, all security systems are based on thoughtful risk management and maximizing the use of resources that can have the biggest impact. No security system is perfect or able to anticipate every potential action, and we need to continue to adapt security protocols to meet new challenges.

Sea-Tac is a perfect example of this truth: Despite all of the measures I just listed, we still experienced a high-profile insider incident just last month.

The need to remain vigilant and constantly improve is why Sea-Tac recently joined in creating a new Industry Working Group on Aviation Security Best Practices. Last month, aviation industry representatives from Airlines for America, Airports Council International-North America, the American Association of Airport Executives, the Cargo Airline Association, the Regional Airline Association, and the National Air Carrier Association met to discuss how we can collectively baseline aviation industry best practices. The group agreed that the best practices identified through this working group should be shared with the U.S. aviation industry, and should also inform the work of the TSA's Aviation Security Advisory Committee's (ASAC) Insider Threat subcommittee. The ASAC subcommittee has committed to incorporating these recommendations into its final report.

As part of the working group's efforts, we are in the process of surveying aviation industry peers about best practices, and hope to have recommendations by the end of this year. Specific topics for investigation include aircraft security, employee training and reward programs, mental health programs, and airport coordination/operation centers. Sea-Tac has also intitiated an independent third-party after-action report of our most recent insider incident, which will contain recommendations for changes that our airport will consider.

I want to close by noting this confluence of activities that are coming together toward the end of the year. In his testimony to the Senate Commerce Committee ear-

lier this month, TSA Administrator David Pekoske shared that he expects ASAC to report back to him by the end of the year on the status of their insider threat recommendations. Combined with the Sea-Tac after-action report, potential TSA and FBI reports on the recent Sea-Tac incident, and the industry working group findings, the aviation community will have an incredible opportunity in early 2019 to thoughtfully discuss opportunities to move forward in impactful ways on insider threat. I look forward to working with this committee and others at that time.

Thank you for your time today, and I welcome any questions you may have.

Mr. KATKO. Thank you Ms. Reiter. There is an awful lot you mentioned that we are going to be following up on. We appreciate that very much.

We applaud you for getting out ahead of the employee screening issue. It is becoming more and more apparent that that is a high priority within our system. There are other things that we are going to be talking about today. One of which I want to talk about at some point is the mental health component. That we need to deal with as well.

The Chair now recognizes Mr. Alterman. He is the president of the Cargo Airline Association where he leads the association in promoting the All-Cargo Air Carrier Industry, formulating industry policy and overseeing the association's daily activities. He has his posse with him behind him today, all the guys from FedEx in those nice uniforms there. I met them out in the hallway.

He is also a senior partner in Meyers and Alterman, a Washington, DC, law firm specializing in air transportation law.

Steve began his career in aviation in 1968 in the Bureau of Enforcement for the United States Civil Aeronautics Board. Initially hired as a trial attorney, he was soon promoted to chief of the Legal Division.

In 1975, he joined the Cargo Airline Association as executive director, and in 1982 took the lead role as president.

We now recognize Mr. Alterman for his opening statement.

STATEMENT OF STEPHEN A. ALTERMAN, PRESIDENT, CARGO AIRLINE ASSOCIATION

Mr. ALTERMAN. Thank you, Mr. Chairman.

Chairman Katko, Ranking Member Watson Coleman, Members of the subcommittee, good morning. My name is Steve Alterman, and I am president of the Cargo Airline Association. As Mr. Katko just mentioned, I started in this in 1968, so I am old. Our organization is a Nation-wide organization representing the interests of the all-cargo industry.

I also have the honor of currently serving as chairman of TSA's Aviation Security Advisory Committee.

I thank you for inviting me today on the insider threat issue.

Before going forward, I would like to thank this committee and the U.S. Congress for what they have done in the reauthorization—actually, the authorization of TSA and those provisions in the FAA reauthorization bill. The provisions in there are long-needed, and we really appreciate it, both from my day job in the Cargo Airline Association and with respect to ASAC.

While the recent incident in Seattle involving the threat and subsequent fatal crash of a Horizon Air aircraft has again raised the issue of insider threats to aviation, the issue is not a new one.

Members of our industry and TSA have for years recognized the need to address this issue.

Accordingly, members of the all-cargo industry have taken steps to deal with the risk by designing and instituting programs that better enable them to recognize potential problems and to devise mitigation strategies.

While these programs are unique to each carrier and are considered proprietary, they all include training in recognizing potentially dangerous behavior, usually coupled with a form of TSA's "See Something, Say Something" program. Some even reward employees who provide information that leads to resolving troublesome issue.

Our member companies, along with our colleagues in the passenger airline and airport industry segments, have continued to work with TSA to develop and build more robust public protections against these threats.

Even though the investigation into the Seattle incident is not yet complete, and we urge everyone to await the findings before drawing any final conclusions, virtually all members of our industry—passenger airlines, all-cargo airlines, and airports—recognize the need to come together to share information, develop a set of recommended best practices, and share those practices among all industry participants. That is the same program that Wendy mentioned in her testimony.

This effort is on-going and it is anticipated that the practices developed will also be shared with the new ASAC Insider Threat Subcommittee that was established in late May of this year.

The Insider Threat Subcommittee replaces and expands upon ASAC's former Employee Access Working Group that made 28 separate recommendations to the TSA for controlling access to the secure area of airports. Many of these recommendations have been instituted and others are in varying stages of development.

As Ranking Member Watson Coleman indicated, one of these programs is the ATLAS program, which is an attempt to make sure that every employee understands that they are likely to be screened or challenged anywhere in the airport during their job.

This is a program that is currently in development. It has been employed in a few areas. It needs to continue that development so that the final goal of employee expectations of screening is accomplished.

In addition, ASAC in a report to the administrator that was sent on July 19 of this year has reviewed existing programs, both in the United States and overseas, to compare existing domestic insider threat initiatives, recognize practices that are common among insider threat programs, and review insider threat mitigation programs at international airports.

The next phase of this project will be to expand the inquiry to make specific mitigation recommendations to the administrator.

This on-going effort will also take into account the specific provisions of the FAA Reauthorization Act of 2018 that is expected to be enacted within the next several weeks.

These provisions include, among others, sections 1933 and 1934 that deal with the requirement to conduct a cost and feasibility

study of airport worker access controls and a review of existing credentialing standards.

To conclude, the issue of insider threats in all segments of our economy is a serious one, and every effort must be made to develop strategies to deter and defeat efforts to harm from within. This effort encompasses both members of the industry individually and between industry and the Federal Government. The all-cargo airlines are committed to this effort, as are our members of the Aviation Security Advisory Committee.

Thank you again for inviting me. I would be happy to answer any questions.

[The prepared statement of Mr. Alterman follows:]

PREPARED STATEMENT OF STEPHEN A. ALTERMAN

SEPTEMBER 27, 2018

Chairman Katko, Ranking Member Watson Coleman, and Members of the subcommittee, good morning. My name is Steve Alterman and I am president of the Cargo Airline Association, the Nation-wide organization representing the interests ofthe all-cargo air carrier segment of the aviation marketplace.[1] I also have the honor of currently serving as chairman the TSA Aviation Security Advisory Committee (ASAC). Thank you for inviting me to testify today on the issue of insider threats to our industry.

While the recent incident in Seattle involving the theft and subsequent fatal crash of a Horizon Air aircraft has again raised the issue of insider threats to aviation, the issue is not a new one for aviation interests. Members of our industry—and TSA—have for years recognized the need to address this issue. Accordingly, members of the all-cargo industry have taken steps to deal with the risk by designing and instituting programs that better enable them to recognize potential problems and to devise mitigation programs. While these programs are unique to each carrier and are considered proprietary, they include training in recognizing potentially dangerous behavior, usually coupled with a form of TSA's "See Something, Say Something" program. Some even reward employees who provide information that leads resolving troublesome issues. And our member companies, along with our colleagues in the passenger airline and airport industry segments, have continued to work with TSA to develop and build more robust protections against these threats.

Even though the investigation into the Seattle incident is not yet complete, and we urge everyone to await the findings of the FBI before drawing any conclusions, virtually all members of the industry—passenger airlines, all-cargo airlines and airports—recognized the need to come together to share information, develop a set of recommended "best practices", and share those practices among all industry participants. This effort is on-going and it is anticipated that the practices developed will be shared with the new ASAC Insider Threat subcommittee that was established in late May of this year.

This Insider Threat subcommittee replaces, and expands upon, ASAC's former Employee Access Working Group that made 28 separate recommendations to TSA for controlling access to the secure area of airports. Many of these recommendations have been instituted and others are in varying stages of development. In addition, ASAC, in a report sent to the administrator on July 19, 2018, has reviewed existing programs both in the United States and overseas to:

- Compare existing domestic Insider Threat initiatives;
- Recognize practices that are common among mature insider threat programs; and
- Review Insider Threat mitigation programs at international airports.

The next phase of this project will be to expand the inquiry to make specific mitigation recommendations to the TSA administrator. This on-going effort will also take into account the specific provisions of the FAA Reauthorization Act of 2018 (H.R. 302) that is expected to be enacted by Congress within the next several weeks. These provisions include, among others, sections 1933 and 1934 that deal with the requirement to conduct a cost and feasibility study of airport worker access controls and a review of existing credentialing standards.

[1] Air carrier members are ABX Air, Inc., Atlas Air, DHL Express, FedEx Express, Kalitta Air, and United Parcel Service Co.

To conclude, the issue of insider threats in all segments of our economy is a serious one and every effort must be made to develop strategies that deter and defeat efforts to do harm from within. This effort encompasses both members of industry individually and between industry and our Government partners. The all-cargo airlines are committed to this effort, as are the members of the Aviation Security Advisory Committee.

Thank you again for inviting me to testify. I would be happy to answer any questions.

Mr. KATKO. Thank you, Mr. Alterman. I appreciate you being here today.

Our third witness is Ms. Lauren Beyer. Ms. Beyer is the vice president for security and facilitation at Airlines for America. In this role, she is responsible for security, cargo, and facilitation issues and works collaboratively with A4A member airlines to advance priorities focused on the safe, secure, and efficient transportation of passenger and goods.

She oversees all aspects of interaction with the Department of Homeland Security, Customs and Border Protection, and the Transportation Security Administration.

Prior to joining A4A, Ms. Beyer served as the director for aviation and surface transportation security at the National Security Council, where she was responsible for planning, directing, and coordinating the development of National aviation security policies.

The Chair now recognizes Ms. Beyer for her opening statement.

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

Ms. BEYER. Thank you.

Good morning, Chairman Katko, Ranking Member Watson Coleman, and Members of the subcommittee. My name is Lauren Beyer. I am the vice president for security and facilitation at Airlines for America. Thank you for inviting me here today to discuss insider threats.

The safety and security of our passengers and employees is our single highest priority. We take aviation security very seriously. We share this common goal with the Transportation Security Administration and work cooperatively and collaboratively with them every day to make sure our skies are secure.

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 in a system that both improves security and facilitates commerce.

We believe that system is best represented through the principles of risk-based security, which is the linchpin and bedrock of our security system today.

One of our Nation's greatest challenges is to strike the right balance between managing risk and overreaction. Enhanced mitigation of insider threats and the efficient operation of our Nation's airports are not mutually-exclusive goals. Government and industry must continue to work together to find pragmatic approaches that appropriately balance these issues.

Insider threat, individuals with privileged access to sensitive areas who misuse this access and compromise security, is of great

concern to the aviation industry. That is why airlines have acted to address this risk.

Some of these measures include enhancements to access control, such as increased CCTV coverage, implementing "See Something, Say Something" campaigns, as my colleagues have already mentioned, providing multiple avenues for reporting of suspicious activity, and offering employee assistance programs.

The tragic incident at Seattle-Tacoma International Airport in August of this year is a somber reminder of the constant vigilance required to keep our skies safe. These kinds of incidents require careful investigation and root cause analysis to determine corrective actions that may be required to mitigate identified security vulnerabilities.

However, the industry is not sitting idly by while the investigation is on-going. In fact, as has been mentioned already, A4A, along with many of our stakeholders partners, has initiated an effort to bring together subject-matter experts from across industry and Government to solicit and thoroughly evaluate airport and aircraft security best practices.

These practices will be shared across the aviation industry and will also inform the work of the ASAC Insider Threat Subcommittee that has already been mentioned. We strongly believe the ASAC is the appropriate venue in which to examine these matters and produce recommendations.

Airlines have worked collaboratively with TSA airports and other stakeholders to implement the 2015 ASAC recommendations to improve employee access controls. Three years later, we applaud TSA and the larger aviation community for implementing the vast majority of those recommendations, and we continue to urge full implementation of those that are still pending.

One aspect of access control that has received much attention is security screening and inspection of employees, and deservedly so. We continue to believe that physical screening of employees is one of several critical elements that should be used in combination to enhance access control.

We applaud the subcommittee, and Chairman Katko in particularly, for his efforts to initiate a study to assess the impact of employee screening.

We are also strong supporters of multiple security layers deployed on a risk-based and unpredictable basis. In this vein, we support further expansion of TSA's ATLAS program.

Other critical elements to guard against insider threats include enhanced and perpetual vetting, security awareness training, as our Ranking Member already mentioned, and intelligence and information sharing.

We continue to urge TSA to expand the list of disqualifying crimes for those seeking a SIDA badge and to align the list of disqualifying offenses with other Government programs. We also urge TSA to extend the lookback period for criminal history records checks.

Finally, this subcommittee knows well that Congress continues to divert a portion of security fees toward general deficit reduction. We continue to request Congress redirect TSA passenger security

fee revenue back to aviation security where those funds could be used to increase TSA capacity to mitigate insider threats.

Our work is never done, and we will continue to evaluate how we can best improve our risk-based system to meet the evolving challenges of aviation security.

Thank you on behalf of our member companies. I appreciate the opportunity to testify, and look forward to your questions.

[The prepared statement of Ms. Beyer follows:]

PREPARED STATEMENT OF LAUREN BEYER

SEPTEMBER 27, 2018

Good morning Chairman Katko, Ranking Member Watson Coleman, 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 insider threats to aviation security.

Overview.—The safety and security of our passengers and employees is our single highest priority. We take aviation security very seriously. We share this common goal with the Transportation Security Administration (TSA) and work cooperatively and collaboratively with them every day to keep our skies safe and secure.

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 every single day. On a daily basis, U.S. airlines——

- Fly 2.3 million passengers world-wide;
- Carry more than 55,000 tons of cargo;
- Operate approximately 27,000 flights;
- Serve more than 800 airports in nearly 80 countries; and
- Directly employ more than 715,000 (full-time and part-time) workers across the globe.

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 in a system that both improves security and facilitates commerce. This becomes even more imperative given the expectation that both passenger and cargo traffic are expected to grow in the coming years. As an industry, we believe that system is best represented through the principles of risk-based security—which is the lynchpin and bedrock of our security system today.

Risk-Based Security.—The administration of risk-based security principles is of paramount importance to aviation security. A risk-based approach recognizes that "one size fits all" security is not the optimum response to threats, including from insiders. Risk-based, intelligence-driven analysis has been a widely accepted approach to aviation security 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 between managing risk and over-reaction. Enhanced mitigation of insider threats and the efficient operation of our Nation's airports are not mutually exclusive goals; Government and industry must continue to work together to find pragmatic approaches that appropriately balance these issues. By utilizing and following risk-based principles we provide a security framework that can be nimbler and more responsive to current and emerging threats and allows TSA and industry to focus finite resources on the highest risks. This framework also takes the operational complexity of the U.S. aviation system into account.

Insider Threats.—Insider threat—individuals with privileged access to sensitive areas, equipment, or information who misuse this access and compromise security—is of great concern to the aviation industry.

That is why carriers have acted to address this risk. A sampling of measures includes:

- Enhancements to access control such as the use of biometrics and CCTV coverage;
- Implementing "see something, say something" campaigns or other challenge programs;
- Providing multiple avenues for reporting of suspicious activity—credited or anonymous—with incentives for such reporting; and
- Offering employee assistance programs addressing issues such as stress management, work-life balance, and grief and loss.

Incident at SEATAC.—The tragic incident at Seattle-Tacoma International Airport in August of this year is a somber reminder of the constant vigilance required to keep our skies safe. These kinds of incidents require careful investigation and root cause analysis to determine corrective actions that may be required to mitigate identified security vulnerabilities. There is much at stake and it is critical authorities thoroughly investigate and analyze all facts.

The industry is not sitting idly by while the investigation is on-going, however. In fact, A4A along with many of our stakeholder partners has initiated an effort to bring together subject-matter experts from across the industry and Government to solicit and thoroughly evaluate airport and aircraft security best practices. These practices will be shared across the U.S. aviation industry. These best practices will also inform the work of the Aviation Security Advisory Committee (ASAC) Subcommittee on Insider Threat previously tasked by the TSA administrator to review and make recommendations to address insider threat more broadly.

Aviation Security Advisory Committee.—We strongly believe the ASAC, of which A4A is a member, is the appropriate venue in which to examine these matters and produce recommendations. 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.

As this subcommittee will remember, in 2015 the ASAC created a working group tasked with analyzing the adequacy of existing security measures and recommending additional measures to improve employee access controls. The effort was supported by the Homeland Security Studies and Analysis Institute (HSSAI), which provided independent and objective subject-matter expertise, as well as by representatives of TSA. That effort produced 28 recommendations for effective measures to protect against possible acts of criminality and terrorism, measures that could be tailored to the unique environment at each airport. Airlines strongly supported and worked collaboratively with TSA, airports and other stakeholders to implement the ASAC recommendations. Three years later, we applaud TSA and the larger aviation community for implementing the vast majority of these recommendations and continue to urge full implementation of those that are still pending. While our work is obviously never done, the guideposts provided by the ASAC recommendations have and will continue to play an important role in improving our risk-based system.

Access Control.—One aspect of access control that has received much attention over the last several years is security screening and inspection of employees, and deservedly so. We continue to believe that physical screening of employees is one of several elements that should be used in combination to enhance access control. We applaud the subcommittee, and Chairman Katko in particular, for his efforts to initiate a cost and feasibility study to assess the impact of employee screening which would include a comparison of estimated costs and effectiveness to the Federal Government, airports, and airlines. We believe that analysis will be critical in establishing how best to move forward and improve access control procedures.

We are also strong supporters of multiple security layers deployed on a risk-based and unpredictable basis. Indeed, the International Civil Aviation Organization (ICAO) recommends increased use of random and unpredictable security measures to contribute to deterrence and to increase mitigation against the potential tactical advantage of insiders. This potential advantage is precisely why flexibility and agility rather than static or predictable processes are key to guard against insider threats. We believe that random and unpredictable checks should be conducted at a frequency significant enough to provide employees with a reasonable expectation that they will be subjected to such checks at any point during their work. That is why we supported the employee screening improvements enacted by Congress in 2016 as part of the Federal Aviation Administration, Safety and Security Act of 2016 (Pub. L. 114–190), which directed TSA to expand the use of Transportation Security Officers to conduct random physical inspections of airport workers in a risk-based manner. TSA leverages its Advanced Threat Local Allocation Strategy (ATLAS) aviation worker screening program to allocate resources for these random inspections, and we support further expansion of the program.

As mentioned, we believe physical screening is only one of several necessary elements to ensure effective access control. Other critical elements include enhanced and perpetual vetting, security awareness training, and intelligence and information sharing. We continue to urge TSA to expand the list of disqualifying crimes for those seeking a Secure Identification Display Area (SIDA) badge as well as to align the list of disqualifying offenses with other Government programs, particularly those of U.S. Customs and Border Protection (CBP). We also urge TSA to extend the lookback period for criminal history records checks.

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 within the TSA, including the September 11 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 $1.6 billion more in TSA security fees—$3.9 billion (2017) 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 to mitigate insider threats, including increased TSA risk-based, unpredictable physical inspections of airport workers at secure area access points and within the secure area.

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

Importance of Commercial Aviation Sector.—Airlines crisscross the country and globe every day carrying passengers and cargo safely and securely to their destinations, and this is an integral part of the economy. In 2014, according to the Federal Aviation Administration (FAA), economic activity in the United States attributed to commercial aviation-related goods and services totaled $1.54 trillion, generating 10.2 million jobs with $427 billion in earnings. As of December 2016, our industry contributes 5 percent of our Nation's GDP. These figures, while both impressive and important, fail to consider the incalculable value of the passengers and crew flying on commercial flights every day. These facts underscore what is at stake and why we need to approach aviation security in a smart, effective, and efficient manner to make sure we get it right. The daily collaboration and communication between TSA and stakeholders will play a vital role toward increasing system-wide protection and lowering risk without unnecessarily clogging up the system.

Thank you, on behalf of our member companies, we appreciate the opportunity to testify.

Mr. KATKO. Thank you very much, Ms. Beyer.

Before we get to Mr. Canoll, I want to note that we are very pleased with the progress that the ASAC as a whole has made. You have expanded your scope and your breadth and your might, and it has become a truly interactive industry leader.

We rely a lot of your findings because we trust them now. Not that we didn't before, but I think the stakeholders you have involved now are really making a difference from a holistic standpoint.

So I really applaud that. I really applaud what Ms. Watson Coleman's bill is going to do for surface transportation, which is out of your purview, but they don't have a similar thing and they need it. They need to have interaction similar to what you have.

So hopefully, if and when that gets formed, you can sit down and do a little cross-pollinating with them. It would be very helpful.

So with that, I appreciate it very much.

We appreciate you being here today, Ms. Beyer.

Our final witness is Captain Tim Canoll. He is the tenth president of the Air Line Pilots Association International. He was elected by the union's board of directors on October 22, 2014, and began his 4-year term on January 1, 2015.

As ALPA's chief executive and administrative officer, Captain Canoll oversees daily operations of the association and presides over the meeting of ALPA's governing bodies, which sets policy for the organization.

He is also the chief spokesperson for the union, advancing pilots' views in the airline industry before Congress, Parliament, Government agencies, airline and other business executives, and also the news media.

Captain Canoll is a Delta MD–88 captain based in Atlanta, having also flown the B727, L–1011, and the B767–757.

The Chair now recognizes Captain Canoll for his opening statement.

STATEMENT OF TIM CANOLL, PRESIDENT, AIR LINE PILOTS ASSOCIATION

Mr. CANOLL. Thank you. The captain forgot to push the button.

Thank you, Chairman Katko, Ranking Member Watson Coleman, and the subcommittee, for the opportunity to be here today. It is my pleasure to represent ALPA's more than 60,000 pilots who fly for 34 airlines in the United States and Canada.

ALPA appreciates Chairman Katko's and Ranking Member Watson Coleman's leadership and the subcommittee's interest in reducing the threat posed by anyone with the intent to harm while working inside our air transportation system.

For decades, ALPA pilots have demonstrated our commitment to aviation security. Our members are highly vetted and trained professionals, who are proud of our contributions to securing our industry.

An insider in aviation is someone with authorization and unescorted access to secured airport areas, such as the security identification display area, known as the SIDA. Such insiders include air crew members, technicians, ground handlers, vendors, as well as law enforcement and security personnel.

Security incidents involving insiders are rare. They can result from malicious intent, complacency, or lack of awareness. The threat includes placement of improvised explosive devices, hijacking, aircraft sabotage. In addition, we are concerned about criminal activity, such as smuggling contraband.

Thanks to the leadership of this subcommittee and the work across our industry, we have made progress in addressing these types of security threats in both passenger and cargo operations. However, the ever-changing threat means we can never rest. We can, and yes, we must do more.

For example, because of regulatory inequity, cargo operations are more susceptible to insider threats, making them a more desirable target for those with malicious intent. Unlike passenger aircraft, many cargo aircraft are not required to be equipped with a hardened flight deck door. Some wide-body aircraft purchased by at least one U.S. cargo operator today don't even have a bulkhead upon which an installed flight deck door could be installed.

Another example, current regulations require cargo aircraft of 100,000 pounds or more to conduct loading and unloading within a SIDA. This means smaller cargo aircraft may be loaded and unloaded outside of a SIDA.

Also of concern is that some foreign nationals and others who are granted access to cargo aircraft cockpits would never be allowed to access the passenger aircraft cockpits. This must change.

In addition, cargo flight crews do not receive equivalent security training for the environment in which they are required to operate.

Airline pilots are equally focused on screening passenger airline operations. We are pleased that the FAA reauthorization, approved by the House and now pending in the Senate, requires secondary cockpit barriers on new passenger airliners.

This good progress for passenger airlines only makes more profound the security inadequacies of flying a cargo flight without a cockpit door, let alone a secondary barrier and a cockpit door.

We are also pleased that the FAA reauthorization included Congressman Katko's legislation that strengthens the SIDA security protocols and requires a system-wide risk assessment of airport access control points and airport perimeter security.

The United States made a quantum leap in aviation security when the TSA adopted a risk-based approach to modernize the one-size-fits-all security that was in place on 9/11. Since then, ALPA has been pleased with the TSA's efforts to seek the perspective of those of us on the front lines of aviation security.

With the continued leadership of this subcommittee, I am hopeful that regulators and industry can act quickly on ALPA's recommendation to require all-cargo operations be conducted in a SIDA, require cargo-specific security training where it is currently inadequate, require fingerprint-based criminal history records checks for anyone with access to a cargo aircraft or that aircraft's cockpit, and require reinforced cockpit doors and adequate secondary barriers on every cargo aircraft.

The Horizon Air incident near Sea-Tac reminds us that, while rare, insider threats exist in both passenger and cargo flight operations. We urge this subcommittee to maintain its oversight and leadership, and ALPA stands ready to continue to work with the airline industry to help ensure that all sectors of commercial aviation are protected from internal and external threats.

Thank you very much. I, too, stand ready to answer any of the committee's questions.

[The prepared statement of Mr. Canoll follows:]

PREPARED STATEMENT OF TIM CANOLL

SEPTEMBER 27, 2018

The Air Line Pilots Association, International (ALPA), represents more than 60,000 professional airline pilots who fly for 34 airlines in the United States and Canada. ALPA is the world's largest pilot union and the world's largest non-governmental aviation safety and security organization. We are the recognized voice of the airline piloting profession in North America, with a history of safety and security advocacy spanning more than 85 years. As the sole U.S. member of the International Federation of Airline Pilots Associations (IFALPA), ALPA has the unique ability to provide active airline pilot expertise to aviation security issues world-wide, and to incorporate an international dimension to security advocacy. ALPA has a long and distinguished record of accomplishments in aviation security which include being a forceful advocate for means to end the hijacking epidemic in the 1960's–1970's, led the development of the Federal Flight Deck Officer program and the Known Crewmember program following the attacks of 9/11, and we have been vocal and active on the issue of the insider threat—the subject of today's hearing—for many years.

BACKGROUND

ALPA sincerely appreciates Chairman Katko's leadership in the aviation security arena and applauds the subcommittee's interests in reducing the threat posed by

anyone who may have nefarious intentions which could be exploited while working inside the aviation system. According to the Department of Homeland Security's (DHS's) September 14, 2018, National Terrorism Advisory System Bulletin, "We continue to face one of the most challenging threat environments since 9/11, as foreign terrorist organizations exploit the internet to inspire, enable, or direct individuals already here in the homeland to commit terrorist acts." Terrorism analysts inform us that according to current intelligence, aviation continues to be the "gold standard" target of terrorist groups, so the timing and subject of this hearing are very appropriate.

For purposes of this statement, we identify an "insider" as someone with authorization and unescorted access to secured areas of an airport and/or aircraft. Certainly, there is potential for insiders employed in positions of trust within the commercial aviation arena to harm passengers, crews, aircraft, and cargo. Fortunately, the number of insider threat incidents is exceptionally low in the United States, but the Government and industry must continually be on their guard against this threat vector and work tirelessly to stay ahead of it.

Aviation security, like many other types of security, is built on a foundation of trust in the individual. Individuals employed in security-sensitive industries, like aviation, must pass extensive background and prior employment checks plus criminal history records checks. Those who pass those checks are issued identification media, access codes and other means to open locked doors, and the scope of their unescorted access is defined according to their job function. Generally, this system works well for the vast majority of trusted employees, but it certainly is not perfect as has been demonstrated on a number of occasions, most recently with an apparent theft and suicide of an airline employee using a company aircraft in Seattle.

THE NATURE OF THE INSIDER THREAT

Fortunately, there are very few incidents of insider attacks against aviation which is a testament to the security systems in place in the United States and most nations around the world. The types of threats that exist can be:

- malicious—the insider seeks to aid or conduct an act which is intended to cause death, injuries, and/or harm to property
- complacent—the insider takes a lax approach to policies, procedures, and potential security risks
- unwitting—the insider is not aware of security policies, procedures, and protocols which expose the organizations/agency to external risks.
- from anyone who has authorized access to the Security Identification Display Area (SIDA) or Air Operations Area (AOA), which includes:
  - Aircrew
  - Technicians
  - Ground handlers (baggage/cargo handlers, gate agents, aircraft servicers, etc.)
  - Vendors (restaurants, construction, transportation, etc.)
  - Law enforcement and security personnel.

In 2014, it was reported that several aviation employees involved in an alleged gun-smuggling ring had been arrested for using commercial airliners to transport prohibited items between two East Coast airports. Even though there was no discernible terrorist threat against commercial aviation, this criminal enterprise created significant concern for the public, Government, and industry. Two other examples of insider threats are as follows:

- In 2013, the FBI successfully established a sting operation in which agents, posing as terrorist co-conspirators, assisted a general aviation avionics technician in bringing what he believed was a bomb onto the tarmac to destroy aircraft. The perpetrator was arrested and ultimately sentenced to 20 years in prison.
- In February 2016, a bomb detonated on Daallo Airlines Flight 159 20 minutes after departing Mogadishu, killing the passenger who had brought it on-board. In May of that year, 2 men were found guilty in court of planning the plot, one of whom was a former security official at the airport, and 8 other airport workers were convicted of aiding the plot.
- In May 2017, an American citizen and U.S. Air Force veteran who had worked as an aircraft mechanic for a U.S. legacy airline and other carriers, was indicted on charges of supporting ISIS and sentenced to 35 years in prison.

In addition to improvised explosive devices, threats from insiders could also come via the use of other prohibited items including firearms, knives, and other types of weapons, plus hijackings. Virtually undetectable threats, however, could come in the form of aircraft sabotage by those with knowledge of aircraft vulnerabilities, or cyber attacks launched distantly. Although airline pilots are focused mostly on the security of ground and in-flight aircraft operations, vulnerabilities to active shooters

and other types of threats from insiders exist within airport terminals and the AOA. As in the case of the 2014 gun-smuggling ring, insiders may also plot and/or carry out criminal activity (e.g., theft) that is not aimed against aviation interests, but is still of concern due to the potential for terrorists to compromise security through the assistance of such actors.

Insider threat vulnerabilities exist in airport terminals, which may be relatively soft targets with large crowds at passenger pick-up and drop-off areas. Other areas which present particular vulnerabilities with congregations of passengers include ticketing/check-in counters, security screening queues, baggage claim areas, and gate areas.

Aircraft are vulnerable to sabotage while on the ground and while in flight. During periods of inactivity, or during off-peak hours at an airport, not all aircraft are parked within SIDAs where multiple security layers are most prevalent. Also, one of the most vulnerable moments during flight happens when the cockpit door is opened and flight crew exit or enter for required rest breaks or physiological needs. ALPA has vigorously advocated for several years for a requirement for installed secondary barriers on passenger aircraft: Lightweight devices, which protect the flight deck from attack during the time that the cockpit door is opened for operational reasons during flight. Airlines are presently permitted to develop their own procedures using service carts and flight attendants to block access to the cockpit when the door is opened, but DHS-conducted testing in the mid-2000's demonstrated the inadequacy of those measures.

Insider threats may also include cybersecurity attacks. We have seen both the operational and financial consequences of the loss of an airline reservation system, or the interruption to ATC services which are computerized. Aircraft are highly computerized machines with the bulk of their systems reliant on electronic primary and back-up sub-systems. With numerous personnel accessing the aircraft while it is on the ground and in the air via Wi-Fi, satellite, or a connected device, the introduction of a malicious virus is a possibility which Government and industry are taking very seriously.

INSIDER THREATS TO ALL-CARGO OPERATIONS

We would like to highlight the security vulnerabilities that exist for all-cargo operations which are distinct from those of passenger operations. All-cargo operations have different regulatory requirements in a number of areas including the following, which make them more susceptible to insider threats:

- The TSA has developed and mandated the teaching of a security training guidance document known as the "Common Strategy" for passenger airlines and crews. The TSA has also established, but not mandated, the teaching of equivalent security training guidance known as the "All-Cargo Common Strategy" for all-cargo airline employees and crews. Government-approved security training, equivalent to that required in the passenger domain, should be required for flight crews and ground personnel supporting all-cargo flight operations.
- In 2003, Congress passed the Vision 100—Century of Aviation Reauthorization Act (Pub. L. 108–176), which included a provision requiring a "training program for flight and cabin crew members to prepare the crew members for potential threat conditions." These provisions were not and have not been required for all-cargo crews; they are needed to help guard against insider and other threats.
- Also, in 2003, Congress passed an appropriations bill (Pub. L. 108–7), which included a provision stating that, "No funds appropriated in this Act may be used to apply or enforce a regulatory requirement for strengthening of flight deck doors" on other than passenger aircraft. That year, the FAA issued a rule requiring flight deck security for all-cargo operations via an installed, reinforced flight deck door or enhanced security measures to screen personnel with access to the aircraft and cargo. It is ALPA's view that flight deck doors are needed on all-cargo aircraft—just as they are on passenger aircraft—as an additional layer of security, and the AMOC needs to be rescinded. Hardened flight deck doors are needed on every airplane, cargo and passenger. That is our best directed deterrent in preventing another 9/11.
- The TSA has developed and mandated the teaching of a security training guidance document known as the "Common Strategy" for passenger airlines and crews. The TSA has also established, but not required, the teaching of equivalent security training guidance known as the "All-Cargo Common Strategy" for all-cargo airline employees and crews. Government-approved security training, equivalent to that required in the passenger domain, should be mandated for and tailored to the needs of flight crews and ground personnel supporting all-cargo flight operations.

- Unlike passenger aircraft which are mandated to be equipped with hardened flight deck doors, all-cargo aircraft are not required to have them unless they had a flight deck door on or after January 15, 2002. However, new, wide-body aircraft are being operated by U.S. all-cargo operators that do not have a flight deck door at all.
- The full all-cargo aircraft operators' standard security plan is written on the basis of an installed, hardened, cockpit door. The plan needs to be updated/amended to reflect the reality of the cargo equipage requirements and reality, and training needs to be required for all affected employees on the plan.
- In 2006, the Transportation Security Administration (TSA) issued new regulations concerning all-cargo operators which created a requirement for those operating aircraft of 100,000 pounds or greater to conduct loading and unloading operations within a SIDA. However, loopholes in the regulations allow part-time SIDAs, and smaller all-cargo aircraft which "feed" cargo to large aircraft to be operated outside of a SIDA at certain airports.
- All-cargo operators have been issued deviations to the Federal Aviation Regulations allowing greater access by non-pilots to aircraft and flight decks. Yet in 2002, the FAA itself referred to the flight deck as "the nerve center" of the operation. The agency further stated that any access request "shall be strictly and narrowly interpreted."
- Some allowed access—which includes foreign nationals with access to the cockpits of some all-cargo transport category aircraft during flight—are vetted on the basis of a Security Threat Assessment (STA), not a fingerprint-based criminal history records check, as is required for insiders within the SIDA.
- The Federal Flight Deck Officer (FFDO) tactics, techniques, and procedures trained by TSA do not reflect the realities of an attack coming on-board an aircraft without a hardened door, and they need to be amended for that purpose. This information has been conveyed to responsible parties in TSA.

ACTIONS TO ADDRESS THE INSIDER THREAT

Commercial aviation has greatly increased its safety record using predictive data which helps identify potential or actual risk. Similarly, TSA and the aviation industry, including ALPA, have been working for several years on the development of more advanced means of predicting if and when a person will become an actual threat to security. The United States has made significant strides toward obtaining a better understanding of the trustworthiness of individuals working in airport sensitive areas, and elsewhere of course, since the 9/11 attacks. This has been accomplished, in part, by the development and use of the FBI's Rap Back service which, as described by the Bureau, "allows authorized agencies to receive notification of activity on individuals who hold positions of trust . . . thus eliminating the need for repeated background checks on a person from the same applicant agency. Prior to the deployment of Rap Back, the National criminal history background check system provided a one-time snapshot view of an individual's criminal history status. With Rap Back, authorized agencies can receive on-going status notifications of any criminal history reported to the FBI after the initial processing and retention of criminal or civil transactions." TSA also performs recurrent checks against the Terrorist Screening Center's watch list and other databases to identify any person who is known or suspected of being involved in terrorist activities.

Perhaps most importantly, TSA has adopted a risk-based approach with the goal of consistently applying it to all aspects of the agency's mission. This replaces the one-size-fits-all security, which was in place on 9/11, and includes consideration of the individual and his or her role within aviation in the development of security requirements and policies. ALPA has been advocating for a risk-based security paradigm for about two decades and has been pleased to work with this committee to improve our Nation's aviation security infrastructure and protocols.

In 2009, TSA initiated an Insider Threat Task Force, and in 2013 created a new Insider Threat Program, which includes an Insider Threat Unit that follows up on threat incidents, inquiries, and tips. Two years later, the agency chartered the Insider Threat Advisory Group (ITAG) of TSA subject-matter experts. Earlier this year, TSA asked the Aviation Security Advisory Committee to create a new Insider Threat subcommittee, on which ALPA participates. The subcommittee has met twice in the past few months and is presently anticipating a request from TSA leadership to expound on and make recommendations concerning the threat posed by insiders with access to aircraft, as was demonstrated in the Horizon aircraft-theft tragedy, along with any new or revised recommendations.

Relatedly, TSA requested ASAC in 2014 to create an Employee Access Working Group, on which ALPA was represented, that delved into the physical screening of

employees at entrances to secured areas and other means of minimizing the risk of insiders. The WG reported its findings to the TSA's leadership the following year along with 28 separate recommendations for improving countermeasures against the potential threats posed by insiders. Those recommendations covered a wide range of different aspects of improvements to thwart the threat and many of them have been implemented, or are in the process of being implemented.

HORIZON AIR TRAGEDY

A matter of great interest continues to be the circumstances of the Horizon Air tragedy near Seattle-Tacoma International Airport, in which a company ramp employee, named Richard Russell, commandeered a Q400 aircraft and after a period of flight, crashed the airplane into the ground. Unanswered questions remain about why this individual committed such an outrageous act, and how he was able to do so. What we know is that the employee is reported to have passed all company and airport vetting checks to obtain employment and required access badges. We also know that he gained access to the aircraft that he eventually stole in an area of the airport in which he was authorized to work unescorted.

MELBOURNE, FL SECURITY BREACH

While not specific to an insider threat, under current deviances for cargo operators, nothing would prevent a security breach like the one in Melbourne, Florida a few days ago from having an impact on cargo security. If there are non-trusted insiders with access because of weak SIDA rules, background checks, and vetting for all cargo operators creates opportunity. This event demonstrates methodology and means, and intent. Additionally, it highlights the ability for people to gain access to SIDAs and it is only a matter of time before they realize that cargo wide-body aircraft have no cockpit doors. Media reports indicate that the individual wanted to do harm with the aircraft. Attempted commandeering seems to be a "trending" risk, which under current rules makes cargo specifically vulnerable.

While we are collectively waiting for the answers which will likely come at some future date, one area of improvement that ALPA believes is worth pursuing is making mental health resources available to all aviation insiders. Since the beginning of this year, ALPA has expended considerable resources on the development of a new, peer-reviewed support program. It is our belief that this program, and others like it, will help save lives of aviation employees and others.

CONCLUSIONS

The insider threat is one that has existed as long as there have been aviation industry employees and one that will be always be a component of the industry. The threat today is manageable, however, because of efforts being made by TSA and the industry to collectively stay abreast of it. However, improvements are needed, particularly within the all-cargo arena which does not have the same level of security as passenger operations. We urge this subcommittee to continue to exercise its oversight and leadership and help ensure that all sectors of commercial aviation are adequately protected from external and internal threats.

Mr. KATKO. Thank you, Mr. Canoll.

I now recognize myself for 5 minutes of questioning, although, since there is not a ton of people here today, we may show a little flexibility to all of us, all of my colleagues.

Just really quickly, Mr. Canoll, I just want to understand this. Is it your testimony that cargo is sometimes unloaded on planes outside of SIDA-controlled areas? How is that possible?

Mr. CANOLL. Well, the way the regulations are crafted, it is measured on a simple weight equivalency. So if the weight of the aircraft is under 100,000 pounds, they don't need to establish a SIDA to load it or unload it. That includes aircrafts like ATR–42s, Cessna 208s, Air Caravans 408s, the new Cessna Sky Caravan. They are all allowed to be loaded and unloaded because they are well under 100,000.

Mr. KATKO. I understand that, but why is that? What is the logic behind that, the size, the weight requirement? How is that possible? I mean, how do you make a determination on what is secure

and what is not based on the amount of cargo? It doesn't make sense to me.

Mr. CANOLL. It doesn't to me either, sir. I agree.

Mr. KATKO. Who makes that decision?

Mr. CANOLL. That, I believe, comes from the TSA. I believe it is from the TSA. But Steve might know better. Steve might know better.

Mr. KATKO. Would you agree that is something we need to address?

Mr. CANOLL. Yes, sir. That is on our list of things that need to be addressed, yes, sir.

Mr. KATKO. OK. Thank you very much.

Ms. Reiter, I appreciate your testimony, everyone's testimony today. As I said in my opening statement, we have documented incidents all over the map here of insider actions, not just threats, actions.

We have a terrorist act in the Midwest, we have individuals willing to smuggle even bombs on airplanes, or at least saying they would be willing to do that. We have individuals that were checking manifests to see where Federal air marshals are.

We have individuals, part of the Dallas/Fort Worth case, we have in the Dallas/Fort Worth case we know that they were seeing where the VIPR teams were, and they were just going in other doors to get into the secure area.

So risk-based security, layered security, of course, is great, but it is not foolproof, obviously.

Mr. Alterman, I am going to get to you in a minute on the ATLAS program, but I do want to talk for a moment with Ms. Reiter.

Based on your experience, we are going to have this report, after-action report, and I would very much like, if it is appropriate, to have it in the secure setting, for both the FBI component, as well as your own after-action report. I think it is really important that we get that in a timely manner.

When do you expect the report to come out?

Ms. REITER. End of year.

Mr. KATKO. OK. Great. So let's try and schedule that as soon as it comes out. I would appreciate that.

But we have talked about the insider threat issue. We have addressed it in the legislation that has been included in the FAA. I am looking very forward to everyone's discussions that are going to be coming out of that bill.

One thing that bill doesn't consider or doesn't overtly consider is what is now a new concern, that is the mental health component. So for anybody here, let's start with Ms. Reiter, how do we address that? What do we do to try and address the mental health component of this threat?

Ms. REITER. Thanks for asking that.

So we are addressing that in our ASAC group as well. We are looking at something that Baltimore currently does, which is not a mandatory issue, but looking at—it is called Mental Health and First Aid, which is offered to any employee that wants to come in and volunteer to look at this program. But it is much of just wanting to come in and talk, someone to talk to, if you will.

We are doing some surveys of how many employers actually offer EAP programs, because maybe they don't offer EAP programs. So we are starting there first, right, and making sure that all the employers offer an EAP program. But just allowing the employees to have an opportunity to have somebody to talk to.

Then, of course, from a legal perspective, can you mandate that people have a mental illness program?

Mr. KATKO. Right. We have to take a look at it.

Ms. REITER. We have to look at that.

Mr. KATKO. My son is in the military. He is a second lieutenant. They have peer-to-peer programs in the military, I believe, from my conversation with Mr. Canoll.

So what about a peer-to-peer type program? If that sounds like a good idea, how would we implement that?

Mr. CANOLL. So in our union, we have great examples of it, and we use it on many of our properties, and we have a National program.

It is not meant to handle the certification medical ability of the pilot to fly, but it is a place for the pilot to go if there are stresses in their life that are affecting their job. We find that if they have a place to go, they are apt to do it instead of internalizing the problem and bringing it into work with them.

Mr. KATKO. It sounds similar to Ms. Reiter's recommendation.

Mr. CANOLL. Exactly. We found it has worked very well, and we will partner with anyone to show them how we are doing it.

Mr. KATKO. OK. Anybody else want to add to that?

Ms. Beyer.

Ms. BEYER. I would just add that, I mean, as has been said, the well-being of our employees is very important to the airlines.

On the point of employee assistance programs, many of the airlines already do offer a number of those programs to address issues such as stress management, or work-life balance, or grief and loss issues, et cetera.

So it is something we are already actively engaged on.

Mr. KATKO. Thank you very much.

Mr. Alterman.

Mr. ALTERMAN. Yes, I would just like to echo what has been previously said. A number of our companies already have programs like that. I think what ALPA is doing is good.

I think that all of these issues will be explored in the context of the Insider Threat subcommittee of ASAC and we will probably come forward with some recommendations on it.

It is a very tough issue because of privacy issues, but it is one that needs to be addressed, and we intend to do it.

Mr. KATKO. I appreciate that. That is going to be important for us to hear from you on. Of course, it is a touchy area.

But here are the facts: Five people now in the country die from suicide. For every suicide, there are 25 suicide attempts. That means several thousand people a day attempt to take their own lives.

In so doing, they often take other people's lives. We see that from the school shootings. We see it in what happened in the Seattle-Tacoma thing, most likely.

So it is an issue that we can't ignore. I am head of the Mental Health Caucus in Congress, and it is stunning to me when we look at the fact that 24-year-olds and younger, the No. 2 cause of death for them is suicide. No. 2. For people, everybody in this country, the No. 10 cause of death is suicide.

So if we don't start embracing the reality that it is here and it is a serious problem and we need to get—I am asking you, and I am sure my colleagues will agree, to take a very deep dive on this as part of your ASAC review. It is going to be very important.

With that, and we will have another round of questions for everybody, but I don't want to take away from everyone's time. Mrs. Watson Coleman has another hearing to get to, so we will have her go next. The Chair will now recognize Mrs. Coleman for 5 minutes or more of questioning.

Mrs. WATSON COLEMAN. Thank you, Mr. Katko.

Thank you each for your testimony. You certainly have raised questions, particularly issues regarding cargo planes and the security necessary. You have made some recommendations that were significant to me in terms of training and the secondary—a door, a door, and then a secondary door, which I am not sure I understand what that is.

Can anyone explain to me what that second?

Mr. CANOLL. So the secondary barrier was part of the 9/11 Commission's report as a companion element to a hardened cockpit door. Knowing that a cockpit door has to be opened at certain types of flights, either for inspections or physiological need, the idea was to ensure that anyone who was outside that cockpit door was barred from rushing the cockpit door when it was opened.

So it is very inexpensive comparatively to airplane things. Screen, mesh screen wire, retractible wire that comes across in front of the door, creates a space between when the cockpit door is open so no one can rush in.

Mrs. WATSON COLEMAN. Oh, I never noticed. Maybe I have not been close enough to first class.

I want to talk about these incidences, though, because these incidences just sort-of scare me.

No. 1 is that with regard to the individual in Washington. First of all, I shared with my Chairman that I want to have a confidential briefing on what we find in this instance as well as the Orlando incident. Very different.

With regard to this incident, I don't know the sort-of cost effectiveness of some kind of vetting that includes some sort of mental health check, whether or not it is on their background or whatever. I don't even know. I don't even know that that would have raised an alarm with regard to this person.

What I think, though, is this whole "See something, say something," if you work with an individual for a period of time and all of a sudden you see different behavior, you see different kind of complaints, you see someone who is very morose or whatever, I think employees need to be alerted to you are not a rat when you share this information with someone who might be helpful to that individual.

I don't know if we are looking at trying to do some employee awareness accountability training now that something like that has happened.

Ms. REITER. So that is also something that we are looking at, but I can tell you that was not this case. The employees were—his employees that were with him were totally shocked. But I can tell you that we are looking at programs such as that where the employees will notice.

Mrs. WATSON COLEMAN. But he got on that plane by himself. My understanding was—and I don't know for sure, this is just information that was shared with me—that, typically speaking, there should have been two people, one with him.

So is that just not enforced? Is that just this incident? What is the deal with that?

Ms. REITER. So I would like to talk more about that in a different setting after the investigation is completely done, if I can, please.

Mrs. WATSON COLEMAN. OK.

I have a question for Mr. Canoll. I mean, how insightful and how like efficient—how does one become a pilot simply because one plays video games that simulate flying? How did that guy get that plane up in the air?

Mr. CANOLL. So if you have a computer with an internet connection and some time, you can download the manuals to just about any aircraft that you want to get familiar with and teach yourself by looking at the panels, "Oh, that is the APU switch, I need to start that first." Download the checklist. It will tell you start the APU, turn on the air conditioning packs, close the cross-feed valves, engage the starter. You could just look at it and figure it out if you had enough time and the desire to do it.

Mrs. WATSON COLEMAN. But that takes some time when you are on a plane, too.

Mr. CANOLL. Well, you could do it, if you could display the panels, a picture of what the overhead panel looks like, that is all you really need.

Mrs. WATSON COLEMAN. I mean, this guy got on the plane, then had to do all the things that you said he did. He got to fly the plane and no one before he got that plane off the ground alerted anybody. Nobody. That is like a lot of time to do something awful like that and not have some kind of checks and balance.

There are so many more questions on this, but I think that there probably are going to be things learned, discussed in different settings.

So in the Melbourne, so what are we supposed to do, electrify fences around airports? What is it that we could have done even in that situation, from your perspective?

Maybe I should ask Mr. Alterman that and Ms. Beyer.

Mr. ALTERMAN. I am not sure I know the answer to that question. I don't know the configuration of the airport. Perimeter security is an issue. It is a serious issue on how we handle perimeter security.

We have just sort-of regenerated our airport and perimeter security subcommittee in ASAC. In view of what happened at Melbourne, I am virtually sure that that subcommittee will be working on that.

I don't have an answer for you. I just have a process for you. We will be looking at that. It is more of an airport than an airline issue. But from an ASAC perspective, it is something we will look at.

Mrs. WATSON COLEMAN. Thank you, Mr. Alterman.

Ms. Beyer, I don't know if you have any——

Ms. BEYER. Sure. I would just add that, of course, it is very important that we allow the investigation to conclude to be able to analyze all the facts.

However, if what I understand about the incident holds true, then I would argue that it reinforces what we believe so strongly in the importance of layered security measures, that it can't just be about perimeter fencing, perimeter security, which is indeed very important, but that can't be the only layer.

As I understand the details of the incident thus far, the two employees that encountered this individual——

Mrs. WATSON COLEMAN. Thank God for them.

Ms. BEYER [continuing]. They used their robust employee training that they had already received to challenge this individual who they didn't believe belonged where he was. I don't believe I have heard that he was badged.

So I think that this is an example of how important those other layers are, a robust challenge culture in the airport for all employees. These are really critical.

Mrs. WATSON COLEMAN. Thank you. My time is up. There are so many more questions that we need to——

Mr. KATKO. You can go ahead and take a second.

Mrs. WATSON COLEMAN. No, I am good. I think that I want to understand were lessons learned and more response to the challenges that we face, particularly in situations like this.

But I also appreciate everything you have said with regard to cargo security. I know we talked about that. We are very interested in ensuring that everything that has to do with aviation, if it is one pilot flying tons of cargo, if it is 700 people on a triple-triple-decker plane, we want to make sure that they are safe.

So thank you so much for your testimony.

Thank you, Chairman.

Mr. KATKO. Thank you very much. There are several more questions I am going to have, so I am going to have a second round for sure.

The Chair now recognize Mrs. Lesko for 5 minutes of questioning.

Mrs. LESKO. Thank you very much, Mr. Chairman.

Thank you for your testimony today. I am a Congresswoman from Arizona. I noticed one of the incidents in 2018, this year, had to do with the FBI doing an undercover operation with some type of drug smuggling, specifically methamphetamines, to several airports, including Phoenix Sky Harbor International Airport.

So my question—one of my questions—is just briefly, if anybody knows, what type of workers were these? Were they a combination of different categories of workers? I am curious if anyone knows that answer.

Mr. CANOLL. No, but I will tell you from a pilot's perspective our concern here is, while this is just illegal transport of contraband,

you would say, well, what is the safety concern for, let's say, the passengers on-board the aircraft? The fact remains there are criminals in the security identification area. If they are willing to do that, what are the other things they are willing to do that could endanger the lives of our passengers or unsecure our cargo?

Mrs. LESKO. Well, yes, I agree, because in the notes that I have not only were they transporting drugs, but also willing to transport guns and explosives. So that is a bit more serious.

I do have a very basic question as well, Mr. Chairman, to anyone that can answer. So for a person that obviously doesn't fly a plane, do all planes like anybody can—I mean, obviously they have to have some type of security clearance, but there is no like code you have to punch in or anything, you just start a plane?

Mr. CANOLL. I will go first.

For those aircrafts in the passenger regime that have a hardened cockpit door, there is an electronic system that unlocks the door to gain access to the cockpit, but not all cargo aircraft have that.

But that door, even when the aircraft is on the ground and being subject to maintenance or cleaning or modification, there are people who have to access the cockpit besides the pilot.

Mrs. LESKO. Sure.

Mr. CANOLL. They will be given that code, too. So there is going to be the proliferation of the code throughout the system.

You can change the code. It is a labor-intensive thing. But that is the only barrier we have now to restrict someone from gaining access to a cockpit that is just sitting there on the ramp.

Mrs. LESKO. Mr. Chair and Mr. Canoll, the code is to the door or the code is to start the plane?

Mr. CANOLL. The code is to unlock the electronic lock to the door to the cockpit.

Mrs. LESKO. OK.

Mr. Chair, I have one more question, and that is a specific question on when is the cockpit door supposed to be closed and who does it? Does the pilot do it? Does the air crew do it? When should it be closed?

Mr. CANOLL. So for passenger operations, and I believe it is specific to the airlines' procedures, for example, at my airline, once the cabin is secured, the lead flight attendant comes to the cockpit, says the cabin is secure. The captain then gives her permission to close the door. She or he closes the door, and then we check the security of the door.

It will remain in that case closed and locked for all purposes, except for physiological needs of the crew or if there is some maintenance need that requires a pilot to go back to check the extension of the landing gear or the condition of the wings during de-icing conditions, until you arrive at the gate and the engines are shut down and the shutdown checklist is complete. Then the cockpit crew will open the door.

Mrs. LESKO. Thank you. The reason I ask that is because I was recently on a flight, and I was kind-of surprised because I used the lavatory right at the front by the cockpit door, and the cockpit door was open and there was a bunch of passengers on-board. We hadn't taken off yet. So I was just curious when do you close the door. I don't know what you mean by when they have cleared the plane.

Mr. CANOLL. So it is when the boarding is complete, the passenger boarding door is closed, and the flight attendants are assured that everyone is in their seats with their seatbelts fastened. That is when the cockpit doors close, before the aircraft moves off the gate for the purpose of going to takeoff.

Mrs. LESKO. Thank you very much.

Thank you, Mr. Chair.

Mr. KATKO. Thank you, Mrs. Lesko.

The Chair now recognizes Mr. Estes for 5 minutes of questioning. I will note that Mr. Estes also got a bill passed as part of the FAA reauthorization, and we are happy for that bill as well.

Mr. ESTES. Thank you, Mr. Chairman.

I have got a couple questions that I wanted probably several people maybe to chime in on. The first one just deals with when an incident happens at an airport or a particular airline notices that, how do the details of the incident and the results and the findings and the action plan for corrective action get communicated through the airport community and through the airline community as well?

Maybe I will just start from an airport standpoint and go from there.

Ms. REITER. Thank you for asking.

So what we did immediately after the incident was contact our associations, ACI and AAAE, and they immediately got a phone call together with all of the airports so that we could talk to the airports about what had happened and we could talk about anything that we felt that we could tighten up at our airport and also that perhaps other airports could glean and help them as well.

We then also contacted A4A, and we got a meeting together with them. That is where we decided that it would be really applicable for us to get a group together to talk about this and also be part of ASAC.

So we also have learned from the events from San Francisco, Los Angeles, and Fort Lauderdale that it made sense for us to do an after-action report because of the event and to hire an outside consultant to do that after-action report. So that is immediately what we had done.

Mr. ESTES. Is that becoming a standard operating practice within the association maybe to communicate that? I mean, just share that information.

Ms. REITER. Yes, it makes sense to go through your associations, yes.

Mr. ESTES. OK. Thank you.

Maybe you can.

Ms. BEYER. Sure. I would just add from the airline perspective, very similar to what my colleague already highlighted, we immediately had calls amongst not only the A4A member airlines, but also our partners at the Regional Airline Association and NACA to discuss the incident so that everyone had the facts about what we knew at that time and what happened and could take any measures that they deemed appropriate.

Also, I think immediate conversation certainly with our TSA partners and other law enforcement officials is very critical.

Mr. ESTES. Thank you.

I don't know if there is anything from a cargo standpoint that might——

Mr. ALTERMAN. I think a couple of things.

No. 1, what you are hearing is very true, and that is the associations within Washington that represent all the segments of the industry work very closely with each other. When something like this happens, believe me, we are on the phone with each other right away.

The other thing, which goes back perhaps one step to your question and it sort-of developed more primacy after the Fort Lauderdale incident, was the question not of the after-action, but what have we learned in terms of when an incident is in progress, who is in charge, who does what, how do we communicate that, how do the various parties, whether it is TSA, law enforcement, airlines, airports, how do they all work together as an incident is happening before we get to the after-action things?

I think there has been a lot of progress in that area, too, because I think a lot of airports—and Wendy can chime in on this—a lot of airports learned that maybe you have got to have one central command center so that when something is happening all the information goes to one place and you have got a process in place. I am not talking about specific things, but a process in place so that while these things are happening there is better coordination among all the people.

Mr. ESTES. All right. Thank you.

Another question that we kind-of talked about in your opening statements is that we are much more engaged in the use of biometrics, particularly as we move forward, and some of the things were just rolling out in terms of how we use that and what do we do.

Are there particular things, have we gotten to the point yet or are we still kind-of in the preliminary stages of, are there additional rules and regulations that need to be put in place for use of biometric, maybe even additional statutory changes that need to be done to allow that effective use?

Ms. BEYER. Sure. So biometrics is a really important issue, as you have correctly noted. You know, I think that I would say, in terms of use in the airports, it can be a very effective tool.

I know, as our colleague Wendy has noted, they use those at employee access points at Seattle Airport. Many other airports have similarly used or implemented biometric systems in a similar fashion.

What works at one airport may or may not work at another, depending on that environment. But certainly it is one effective tool.

Mr. ESTES. Thank you.

Ms. REITER. Yes, I would say I agree with Lauren. It is very successful for us. However, it is based on layers of security for different airports. So it is very successful for us.

Mr. ESTES. All right. Thank you.

Mr. Chairman, I yield back.

Mr. KATKO. Thank you. You will have an opportunity for a second round, Mrs. Lesko and Mr. Estes, if you are so inclined.

I have several questions, no particular order of importance. But as I think about all this and I think about all the efforts that are

going on in the United States, obviously, I think our airports do an extraordinary job of protecting people, but it is our job to constantly probe the vulnerabilities and help you address them.

I am wondering if anyone has an opinion on what they see, for example, in the Caribbean, which I think is an often very ignored part of our air traffic as far as security issues. But somebody was talking about breaching the fence and what goes on. I remember landing in Caribbean airports, I don't ever see a fence, or if it was, it was minimal.

So I would like to hear does anyone have security concerns about what is going on in the Caribbean Basin airports?

Ms. BEYER. So I guess how I would approach that would be there are, of course, a number of our airlines that operate many flights in the Caribbean. There are two important pieces of that puzzle from a U.S. perspective. I think one, of course, is TSA responsibilities for assessing those airports. In certain cases, not just in the Caribbean, in other places of the world, they then impose additional requirements when they believe the security is not adequate.

But I would also add that in many instances, not necessarily specific to the Caribbean, in fact at all locations where airlines operate overseas, we conduct our own risk assessments of those airports and the particular dynamics in that environment, and in many instances may choose to, on our own accord, implement additional security requirements around our aircraft, passengers, cargo, et cetera, to ensure that anything put on-board our aircraft en route to the United States is secure.

Mr. KATKO. We are contemplating a review, first-hand review of those airports, because there are some concerns from the security standpoint that I think need to be addressed. So if you feel more comfortable talking about some of these in a secure setting, I am happy to hear that. But I am just trying to get a general feel whether there are some concerns about those airports.

Anybody else want to offer anything?

Mr. ALTERMAN. Not necessarily with the Caribbean airports. A lawyer never does this, but I don't know.

But I think what Lauren said is very true about international operations. We all try to base our judgments in what we do based on the risk inherent in any particular operation. When we are operating from dangerous areas or from airports that have a security that is less than others, we take extraordinary steps to make sure those are secure.

Freight moving into the United States is given much more security when they come from an Afghanistan than they do from an Iceland. We are always looking at the risk inherent in operating in various places, and the measures we take are tailored to those risks.

So if there are problems in the Caribbean, and I don't know of exactly what those are, I am sure our operators do and are taking the steps. All of our security programs are in force in all of those places.

Mr. KATKO. OK. Thank you.

I am going to switch gears here a bit. I know we are going to study this, we are going to get an after-action report, we are going to get all the discussions down the road. But the fact remains is

a maintenance worker walked into a plane, started it up, and took off. Is there something we can do now to kind-of prevent a possible copycat from happening between now and the time we get your detailed input?

I mean, how it is that a ground guy can walk up into a plane and turn it on and take off? I mean, forgive my ignorance, are there any biometrics that help you with the plane? Who has access to the plane? Is that something that is of concern? There are not even keys to planes.

Also I understand that in this particular instance the individual was getting some training within the airport for flying, if I am not mistaken, having access on his down time. I am just curious about all of that.

So I don't know who wants to start with that. That is a lot of stuff there to cover.

Mr. CANOLL. So I will start, Mr. Chairman.

As mentioned before, there isn't any key to the airplane or any biometric loop you have to check off before you——

Mr. KATKO. Not just cargo, any airplane, right?

Mr. CANOLL. Any airplane. They are just not designed that way.

But there are things that the industry groups are working on that are relatively quick to implement. Most of them we can't really discuss here because it would disclose what the countermeasure would be. But some are very simple, like blocking access to the runway once there is an unauthorized movement on the aircraft. It is relatively simple. You can say it, but, of course, the configuration geometry at each airport might be different. If there is a ramp very close to the airport, you may not have time to block the access to the runway.

But those are the ideas that are being bantered about. I think there are some solutions. It is not going to be fool-proof, but it is going to be a really good layer to prevent this from happening again.

Mr. KATKO. Does anybody else want to add to that?

Ms. BEYER. Go ahead, Wendy.

Ms. REITER. Sorry, Lauren.

So to talk a little bit about this particular case. First of all, he was viewing the simulation of this particular aircraft in the break room on several occasions, so he did clearly understand—or wanted to understand how to fly this aircraft. He was not a pilot by any means and this is how he learned how to fly the aircraft.

The aircraft was extremely close to the runway. It was at the north end of the airfield that was very close to our runway. From the time that he got into the airplane—by the time that he started the engines, pushed the aircraft back, and got into the air was less than 4 minutes. So it was extremely close to the airfield.

There are multiple things that we have done to increase or to make security more visible since then. We have more uniformed and nonuniformed personnel down at that end of the airfield. It is quite remote comparatively.

We also are looking at other technologies. You know, perimeter. There is some video technology that you can purchase for a fence line that we are currently looking at to have done within the next 6 to 8 months. Rap Back is another, which would not have helped

us in this case because he didn't have anything in his background anyways. However, the next case it could help us, right? So there are other things that we are doing to help as well.

Alaska Airlines, it has increased their "see something, say something," have met with every single one of their employees to talk about if you see something that is not the same or out of the ordinary, or if you see an employee that is acting differently, please alert us. Stop the operation. It is OK to stop the operation if you see something.

So we definitely have increased our visibilities, and so has Alaska Airlines and other airlines, for that matter.

Mr. KATKO. Just out of curiosity, why was a flight simulator for that particular plane in a break room?

Ms. REITER. He was viewing it on one of the computers in the break room.

Mr. KATKO. Oh. So, in other words, he just had access over the internet to it.

Ms. REITER. Right.

Mr. KATKO. Oh, I gotcha. OK. OK. I thought it was like "here is how to fly this plane" in a break room.

Ms. REITER. No. No, not at all.

Mr. KATKO. Whew. OK. All right. We are good.

All right. Thank you.

Anybody else want to add anything?

Ms. BEYER. I would just add to Wendy's point, the airlines operating in Seattle have worked very closely with Wendy and her team on a number of the short-term changes that she already outlined. But some of the airlines have also implemented their own measures, such as increased police or management presence around aircraft, particularly at remote locations.

I would just say I firmly believe, though, while it is important to evaluate the facts of individual incidents, that we shouldn't just focus on the one or two incidents. I believe our approach should be to evaluate insider threats globally. Airlines, as I know airports do as well, the airlines already have robust insider threat programs that are tailored to the unique needs of their companies.

That being said, we are constantly evaluating how we can be better and if we need to change some of our practices, and that is why we initiated the working group that has been mentioned a lot today, and that is why we are actively participating in the ASAC effort.

Mr. KATKO. I think the ASAC effort is going to be critically important. You have a long list of things to look at. I mean, if this bill gets signed, gets through the Senate, it is going to direct you to do that.

So, I mean, I look at the mental health component, which I am asking you to specifically take a look at. The ground component. How do you stop a plane if it is going to go? Is blocking a technique to be used? Plane access. Who is getting access? Why? What are best practices for that?

Then, in addition to all the other access control issues, like the smuggling, let's not forgot something this size can take down an airplane now. We know that. It is going to take an awful lot of really good, hard critical thinking to fix that. We have gaps that are

gaping, and a lot of it is from the insider threat perspective, that we keep an eye on.

So I hope and pray that you are going to do a very thorough report on this because we are definitely going to have to talk more about this.

Mr. ALTERMAN. Yes. Thank you, Mr. Chairman.

We are, and I hope we can do the good job. I think that we have the right people in the room on the new Insider Threat subcommittee. We are looking at all the issues you mentioned. We are looking at the requirements from the FAA Act when it is passed.

We understand the seriousness of it. We have a very good TSA team working with us. They have something called the ITAG that they have had for several years, which is the Insider Threat Advisory Group. That has now been rolled into the—not rolled into, but is cooperating with and working with the ASAC team on this so that we now have all the information we hope in one place.

Several meetings have been held already, and we hope to get something by the end of the year. This is difficult. Once you even decide what to do, writing a report and getting it through everybody is difficult. But we understand that.

I might say, sort-of as an aside, I actually counted, and the FAA bill has 9 separate tasks for ASAC, and 2 or 3 others that relate to the work we are already doing. We understand that, and we appreciate your confidence in us. We may need mental health training for all the ASAC members before we are through.

But thank you.

Mr. KATKO. Listen, that is part of it. Your credibility has skyrocketed because you are producing, and you are collaborating. You take into account everyone's concerns. From that come good things. I think we could learn in Congress from that, to be quite frank with you.

So it is something that is going to take an awful lot, but I can't think of a more important issue for the airline industry right now than this. We are doing a pretty good job of securing things.

The other big thing I can think of is 3-D scanners. How are we going to get those to the front line fast enough? We are going to have to think outside box on that, but that is for another day.

But I do have a follow-up question for you, Mr. Alterman. That is, I know TSA and ASAC's current actions are relating to insider threat. You have been doing something with them, I believe it is a two-part task that Administrator Pekoske has come to talk to you about. Could you describe for a little bit what that is and where you are with it?

Mr. ALTERMAN. Yes. We received a tasking from the administrator to do basically a two-step process. The first step in that was basically a research project. That project was finished and delivered to the administrator on July 19 of this year. It involved looking, as far as we could in the time frame allowed, at not only what domestic people are doing on insider threat, what are some of the practices they are doing, but also looking overseas at various airports and trying to determine, to the extent that they would talk to the committee, to determine what is going on internationally that might inform us on what we are doing.

That report was submitted to the administrator on July 19. I was hoping that perhaps I could just attach it to my testimony, but I am not sure it has been made public.

Mr. KATKO. It hasn't been made public, and I am wondering why.

Mr. ALTERMAN. I have no idea.

Mr. KATKO. It is not yours to answer. We are going to have to talk to Mr. Pekoske.

Mr. ALTERMAN. Yes. I don't think there is anything in it that is SSI, frankly. But I think it might be useful for you to understand the depth of that report to get it from——

Mr. KATKO. That would be great.

Mr. ALTERMAN. I just feel unconformable giving it to you without the authority to do it.

Mr. KATKO. I understand. We will get it from him.

Mr. ALTERMAN. The second part, the second tasking, which we think we know what it is going to say but we haven't yet formally received from the administrator, is looking at what the research was. What are the next steps? How do we define the mitigation efforts that we might take based on what we have already learned?

That has gone over to the Insider Threat subcommittee to start working on even though we don't formally have the letter. That involves access controls. It involves all the things we have talked about this morning.

Mr. KATKO. It dovetails with what is going to be in the FAA bill as well. So that is good you are going to jump on that.

Mr. ALTERMAN. Yes. Exactly.

Mr. KATKO. That is encouraging. Good.

I understand the position you are in and I am not going to ask you to disclose it. But we will have a discussion with Mr. Pekoske, and I am sure we will come to a conclusion on that.

The Chair now recognizes Mrs. Lesko for as many questions as she wants to ask. We have some flexibility here.

Mrs. LESKO. Mr. Chairman, I have no more questions.

Mr. KATKO. OK.

Is there something, as long as we have a few minutes, is there something that you wanted us to bring up that we haven't brought up? I am asking any of the witnesses.

Mr. CANOLL. So I just want to emphasize one element here. If you are viewing the entire global view of insider threat, I really want to emphasize for the committee the soft underbelly, in our opinion, is the disparate regulations within the cargo world.

If you are looking to do something evil with a jumbo wide-body aircraft—and I want to be clear, most of the jumbo wide-body aircraft in the United States are cargo aircraft. They are cargo and not passenger aircraft. Many of them, soon to be hundreds of them, are going to be flying around without cockpit doors.

All of our tactics, procedures, and policies are built around defending that cockpit with a cockpit door. There are no published procedures or training for how do you defend the cockpit without a cockpit door.

As a reminder, these cargo aircraft are not all-cargo. They have people on board. They have animal handlers, couriers, other employees on board with unfettered access to the pilots at the controls of the aircraft at any given moment.

So we need to do some serious thinking about that vulnerability, because, in our opinion, that is by far the most critical one. It is growing. It is not just a static vulnerability we see today. There are hundreds of aircraft being delivered in this configuration in the future. This vulnerability will grow over time.

Mr. ALTERMAN. Mr. Chairman.

Mr. KATKO. Yes.

Mr. ALTERMAN. May I respond?

Mr. KATKO. Sure.

Mr. ALTERMAN. I hadn't planned on it, but I need to respond to that.

Mr. KATKO. Sure.

Mr. ALTERMAN. We love our pilots. They are very professional. We work tremendously with ALPA on a bunch of issues. They are simply wrong on this one.

Let me explain the hardened door, because I just want to put it in the record so it is not a one-sided—I don't want to have an argument here. It is not appropriate.

Mr. KATKO. I understand.

Mr. ALTERMAN. The all-cargo industry has a completely different operational model than the passenger industry. Our security are designed around that operational model.

We don't carry passengers in any normally accepted use of that term. We do carry individuals, very limited amount of individuals. If there is any inference that we are not regulated in the security of the cockpit, that is incorrect.

We do two things. No. 1, the regulations require us to screen for stowaways, and we do that. We haven't found any. We continue to do that. But directly with what Captain Canoll has said, the regulations require that the all-cargo industry either have an installed door or have a program, an alternative program, that is approved by TSA. All of them have that program.

It is important to note that these alternative procedures that are applied that protect the plane against the limited individuals that are on there, whether they be other pilots, whether they be animal handlers, whether they be couriers, they are extensive, they have proved effective. Each company may have a different procedure to deal with it. But all of them include extensive background checks of every passenger that gets on that plane and extensive screening of every passenger on that plane.

In fact, the only incident that I know of that has developed on a cargo plane in recent years has been a deranged pilot. That is not to say anything bad about pilots. But we have been operating millions of flights over many years and have never had a problem there. We are regulated.

I just wanted to put that on the record. I don't want to have a debate with Mr. Canoll.

Mr. KATKO. I appreciate it. This is not what we are here for, to have a debate. But, I mean, I guess he is calling into question the adequacy of the current TSA regulations, and we will take a look. You are welcome to follow up with us in writing.

Mr. CANOLL. Steve and I have had that debate many times.

Mr. KATKO. I understand. I understand completely.

Mr. ALTERMAN. Usually over a beer.

Mr. KATKO. That sounds good.

Anything else anyone wants to add that we haven't discussed?

I do appreciate the frankness of Ms. Reiter to come here based on a tough situation. As always, she displays a tremendous amount of professionalism, as have all of you. So I appreciate all your candid testimony today.

Listen, we are all on the same page here. We are all just trying to keep people safe, keep pilots safe, keep airplanes safe, keep our country safe.

It is our duty to do the oversight. We are going to continue to do it. We have an extraordinary number of hearings in the subcommittee because we take it very seriously. But we do appreciate the collaborative nature, and we appreciate the input of all of you.

So with that, the hearing remains—I have magic words I have got to say here. Excuse me a second. This is what happens when you go off script.

Members of the committee may have some additional questions and we will ask you to respond to those in writing. Pursuant to Committee Rule VII(D), the hearing record will be held open for 10 days.

Without objection, the subcommittee stands adjourned.

[Whereupon, at 11:24 a.m., the subcommittee was adjourned.]

APPENDIX

QUESTION FROM HONORABLE BRIAN K. FITZPATRICK FOR TIM CANOLL

Question. Captain Canoll, given the security discrepancies between security for passenger versus cargo operation at airports, is there a real risk associated with cargo operations that we are overlooking?

Answer. Response was not received at the time of publication.