UNDERSTANDING THE CYBERSECURITY OF AMERICA'S AVIATION SECTOR

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY AND INFRASTRUCTURE PROTECTION

AND THE

SUBCOMMITTEE ON TRANSPORTATION AND PROTECTIVE SECURITY

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

SEPTEMBER 6, 2018

Serial No. 115–75

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

34–446 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*
KATY FLYNN, *Deputy General Counsel*
HOPE GOINS, *Minority Staff Director*

SUBCOMMITTEE ON CYBERSECURITY AND INFRASTRUCTURE PROTECTION

JOHN RATCLIFFE, Texas, *Chairman*

JOHN KATKO, New York
DANIEL M. DONOVAN, JR., New York
MIKE GALLAGHER, Wisconsin
BRIAN K. FITZPATRICK, Pennsylvania
DON BACON, Nebraska
MICHAEL T. MCCAUL, Texas *(ex officio)*

CEDRIC L. RICHMOND, Louisiana
SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
VAL BUTLER DEMINGS, Florida
BENNIE G. THOMPSON, Mississippi *(ex officio)*

KRISTEN M. DUNCAN, *Subcommittee 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

UNDERSTANDING THE CYBERSECURITY OF AMERICA'S AVIATION SECTOR

Thursday, September 6, 2018

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

The subcommittees met, pursuant to notice, at 10:08 a.m., in room HVC–210, Capitol Visitor Center, Hon. John Ratcliffe [Chairman of the Cybersecurity and Infrastructure Protection subcommittee] presiding.

Present: Representatives Ratcliffe, Katko, Donovan, Gallagher, Fitzpatrick, Bacon, Lesko, Watson Coleman, Keating, Langevin, Payne, and Demings.

Mr. RATCLIFFE. Good morning. The Committee on Homeland Security, Subcommittees on Cybersecurity and Infrastructure Protection and Transportation and Protective Security will come to order.

The subcommittees are meeting today to receive testimony regarding the cybersecurity posture of this Nation's aviation sector. I now recognize myself for an opening statement.

I am grateful to be holding this hearing this morning with my good friend and Chairman of the Transportation and Protective Security Subcommittee, John Katko. I want to thank him for convening this hearing with me today to examine a topic that I think fits hand-in-glove with the security of our Nation.

I have always said that cybersecurity is National security. There is no better example of that than in the aviation industry. When we think of threats to the industry, traditional avenues of attack are what first come to mind. These threats, like hijackings and bombings, will continue to pose a major security concern moving forward.

However, as devices, aircraft, and systems become more interconnected, cybersecurity will increasingly play a larger role in aviation security. That is because nation-states, cyber criminals, and hacktivists all possess an incentive to manipulate systems within this sector. Whether it be looking to gain a competitive advantage, or financially motivated actions, or simply a political statement, the space will always be crowded by malicious actors seeking to do us harm.

That is why we need to understand all avenues of attack, to prioritize their severity and to mitigate those vulnerabilities as quickly as we can.

Innovation has brought increased efficiencies to daily life, but it has also tied together networks like we have never seen before. Therefore, this is not a single-minded task. We cannot be narrow in our focus. We have to explore the entire aviation ecosystem as a whole.

If we have a single weak link anywhere along the chain, then the entire chain can fail, like earlier this year, when we saw a ransomware attack which targeted the city of Atlanta and forced Hartsfield-Jacksonville Atlanta International Airport to turn off its WiFi services for hours. That is one of many examples I could give to illustrate the cross-cutting nature of the sector.

All of these pose inherent logistical, financial, and security concerns. It therefore becomes incumbent upon the Department of Homeland Security, Congress, and the private sector to work together to find ways to create resilient systems, to create redundancies, to share threat information, and to build safety and trust into systems that have become integral to American travel.

Trust is instrumental in the continued health of the aviation industry. Customers and travelers need to have faith in the systems they are using, whether it be from the information on arrival and departure boards to security on the airplanes themselves. Losing the trust of the everyday American would be disastrous for the sector, and gaining it back would be an uphill battle.

Fortunately, safety has always been an overriding concern of the aviation industry. The industry has typically and generally risen above all others in this case. Safety has been culturally built into this sector over time. The lessons learned from 9/11 have matured both private-sector and Federal Government entities to the point they are at today.

However, we still need to clearly delineate roles of entities like NPPD, TSA, and the FAA, which we have come to rely upon for our security concerns. We have to build partnerships both within the private sector and within the Government, partnerships like the Aviation Cyber Initiative, which brings together Government stakeholders from DHS, DOT, and DOD to tackle cybersecurity problems across the aviation sector. It provides auditing on a voluntary basis to further the goal of a safer, more secure ecosystem.

DHS's National Protection and Programs Directorate recently announced the creation of a National Risk Management Center in its effort to enhance risk management integration across the public and private sectors. I am very interested in the rollout of the center and hope it will become another essential tool for the public-private collaboration based on and focused on cybersecurity.

By leveraging existing practices and partnerships already in existence, the aviation industry can maximize security benefits. A 2016 study found that 91 percent of airlines are planning to invest more in cyber programs over the next 3 years, which is up from only 41 percent back in 2013. That is good news.

Stakeholders remain poised to tackle the issues at hand and ensure a safe cyber ecosystem within their sector. It is my hope that

organizations like DHS's NPPD are offering support that is beneficial to this sector.

In our continued efforts to support the work and mission space of NPPD, I want to remind my colleagues that late last year, the House passed H.R. 3359, the Cybersecurity and Infrastructure Security Agency Act, a bill that is essential to solidifying and strengthening DHS's cybersecurity mission and which would support NPPD's efforts to bolster aviation cybersecurity.

I am excited to explore the issue of aviation cybersecurity today. I have faith that all parties will rise to the occasion and ensure that the American people can always have trust in the cybersecurity within the aviation sector.

I want to thank the witnesses for their time and for being here today. I very much look forward to their testimony.

[The statement of Chairman Ratcliffe follows:]

STATEMENT OF CHAIRMAN JOHN RATCLIFFE

SEPTEMBER 6, 2018

I am glad to be holding this hearing with my good friend, and Chairman of the Transportation and Protective Security Subcommittee, John Katko. I want to thank him for convening this hearing with me today to examine this topic that fits hand-in-glove with the security of our Nation.

I have always said that cybersecurity is National security. There is no better example of that than in the aviation industry.

When we think of threats broadly to the industry, traditional avenues of attack are what first come to mind. These threats, such as hijackings and bombings, will continue to pose a major security concern moving forward. However, as devices, aircraft, and systems become more interconnected, cybersecurity will increasingly play a larger role in aviation security.

Because nation-states, cyber criminals, and "hacktivists," all possess an incentive to manipulate systems within the sector.

Whether it be looking to gain a competitive advantage, a financially-motivated action, or simply a political statement, the space will always be crowded by malicious actors seeking to do harm.

This is why we need to understand all avenues of attack, to prioritize their severity, and mitigate those vulnerabilities as quickly as we can.

Innovation has brought increased efficiencies to daily life, however, it has also tied together networks like we have never seen before. Therefore, this is not a single-minded task. We cannot be narrow in our focus, as we must explore the entire aviation ecosystem as a whole.

We cannot have a single weak link across the entire chain, or else it could all fail.

For example: A ransomware attack which targeted the city of Atlanta earlier this year forced Hartsfield-Jackson Atlanta International Airport to turn off its Wi-Fi services for hours. This is one of many examples illustrating the cross-cutting nature of the sector. All which pose inherent logistical, financial, and security concerns.

Therefore, it becomes incumbent upon the Department of Homeland Security, Congress, and the private sector to work together to find ways to create resilient systems. To create redundancies. To share threat information. And to build safety and trust into systems that have become integral to American travel.

Trust is instrumental in the continued health of the aviation industry. Customers and travelers need to have faith in the systems they are using, whether that be arrival boards or the airplanes themselves. Losing the trust of the everyday American would be disastrous for the sector and gaining it back would be an uphill battle, as we cannot explicitly see increased firewall protection, for example.

Furthermore, safety really is key as well. The aviation industry rises above all others in this case, as safety has been culturally built into the sector over time. The lessons learned from 9/11 have matured both private-sector and Federal Government entities to the point that they are at today.

However, we need to clearly delineate rolls of such entities as NPPD, TSA, and the FAA which we have come to rely on for our security concerns.

We must build partnerships both within the private sector and within Government. Partnerships such as the Aviation Cyber Initiative, which brings together Government stakeholders from DHS, DOT, and DOD to tackle cybersecurity problems across the aviation sector. It provides auditing on a voluntary basis to further the goal of a safer, more secure ecosystem. DHS's National Protection and Programs Directorate recently announced the creation of a National Risk Management Center, in its effort to enhance risk management integration across the public and private sectors. I am very interested in the rollout of this Center and hope that it will become another essential tool for public-private collaboration focused on cybersecurity.

By leveraging existing practices and partnerships already in existence, the aviation industry can maximize security benefits. A 2016 study by SITA found that 91 percent of airlines are planning to invest in cyber programs over the next 3 years, up from only 41 percent in 2013. Stakeholders remain poised to tackle the issues at hand and ensure a safe cyber ecosystem within their sector, and it is my hope that organizations like DHS's NPPD are offering support that is beneficial to this sector.

In our continued efforts to support the work and mission space of NPPD, I want to remind my colleagues that late last year, the House passed H.R. 3359, the Cybersecurity and Infrastructure Security Agency Act, a bill that is essential to solidifying and strengthening DHS's cybersecurity mission and would also support NPPD's efforts to bolster aviation cybersecurity.

I am excited to explore the issue of aviation cybersecurity today. I have faith that all parties will rise to the occasion and ensure that the American people can always have trust in the cybersecurity of the aviation sector.

I want to thank the witnesses for their time and I look forward to their testimony.

Mr. RATCLIFFE. The Chair now recognizes the gentlelady from New Jersey, Ms. Watson Coleman, the Ranking Member of the Transportation and Protective Security Subcommittee for any opening statements she may have.

Mrs. WATSON COLEMAN. Thank you very much, Chairman Ratcliffe and Katko and my fellow Ranking Member, Mr. Richmond, who will be here, for holding today's hearings.

Thank you, Mr. Porter and Mr. Troy and Mr. Stephens, as being our witnesses here today.

I am very glad we are holding this hearing, because it seems to me that the topic of aviation cybersecurity has not received the attention it demands. Threats to the transportation sector are constantly evolving and efforts to secure transportation must be beyond simply reacting to the most recent attempted attacks.

Next week, we will commemorate the 17th anniversary of the September 11 attacks. One reason terrorists were able to carry out such deadly attacks on that day is that they took us by surprise. The U.S. aviation sector was vulnerable because security efforts had not focused on the possibility of terrorists hijacking a plane and using the plane itself as a missile.

In the years since then, we have invested heavily in aviation security by hardening cockpit doors, creating a TSA, improving passenger and baggage screening, and refining intelligence-sharing and vetting processes. These efforts have unquestionably made air traffic more secure, but we cannot let our guard down now. We must urge security agencies to think creatively about potential new attack vectors, as terrorists continue to search for vulnerabilities to target.

With that in mind, we must do more when it comes to the cybersecurity or transportation systems. Seventeen years after terrorists gained access to cockpits via physical means, we cannot allow them access to cockpits via cyber means. I must have a mouthful of marbles today.

Last fall, reports emerged that a research team led by DHS Science and Technology Directorate was able to remotely hack into the systems of a commercial passenger jet. As a matter of fact, as a part of my briefing, I was informed of three additional opportunities that were used to try to hack into systems, even those involving the notorious Russia.

In the wrong hands, such a capability could result in mass casualties. Even a much less drastic security breach could have major consequences. The aviation sector relies on a vast network of interconnected systems, including air traffic control, airports, airline, operation systems, and reservation and ticketing systems. A cyber attack against any one of these could cause chaos and confusion, resulting in canceled flights, diminished consumer confidence, and enormous cost to the airlines and airports.

Despite the clear vulnerabilities and the consequences of a cyber attack with the aviation sector, not much has been done to improve cybersecurity. Although TSA requires the airports and airlines to adopt and implement security programs covering a wide range of measures to protect against attack, TSA does not require these programs to include any cybersecurity measures. Instead, TSA only shares a list of recommended best practices for airports and airlines to implement at their discretion.

It is clear that we need the investment on the part of the Government and research and development on what to do when we find these intrusions to take place, not just to identify them, categorize them, ensure them, but how do we stop them, should they become a threat?

When it comes to securing air travel, voluntary measures are just not enough. That is why I am working with my colleagues to develop legislation to require TSA to issue new rules to airports and airlines requiring implementation of baseline security measures, some of which may also apply to surface transportation systems, as well.

Additionally, while this hearing is focused on the aviation sector, I would be remiss if I didn't note that these issues do, indeed, affect other modes of transportation, as well. Mass transit passenger rail, freight rail, and pipeline systems all rely on networks that must be secured against cyber attacks. It is my hope that today's hearing will provide us with more information on current cybersecurity efforts within the aviation sector and what work remains to be done.

Again, I want to thank the witnesses for joining us. Thank you, Chairmen, for bringing this hearing to us today. I yield back the balance of my time.

[The statement of Ranking Member Watson Coleman follows:]

STATEMENT OF RANKING MEMBER BONNIE WATSON COLEMAN

SEPTEMBER 6, 2018

Thank you to Chairmen Ratcliffe and Katko, and my fellow Ranking Member Richmond, for holding today's hearing.

Thank you also to our witnesses for being here today to share your expertise with us.

I am really glad we are holding this hearing because it seems to me that the topic of aviation cybersecurity has not received the attention it demands.

Threats to the transportation sector are constantly evolving, and efforts to secure transportation must go beyond simply reacting to the most recent attempted attacks.

Next week, we will commemorate the 17th anniversary of the September 11 attacks.

One reason terrorists were able to carry out such deadly attacks on September 11 is that they took us by surprise.

The U.S. aviation sector was vulnerable because security efforts had not focused on the possibility of terrorists hijacking a plane and using the plane itself as a missile.

In the years since then, we have invested heavily in aviation security by hardening cockpit doors, creating the TSA, improving passenger and baggage screening, and refining intelligence-sharing and vetting processes.

These efforts have unquestionably made air travel more secure, but we cannot let our guard down now.

We must urge security agencies to think creatively about potential new attack vectors, as terrorists continue to search for vulnerabilities to target.

With that in mind, we must do more when it comes to the cybersecurity of transportation systems.

Seventeen years after terrorists gained access to cockpits via physical means, we cannot allow them to gain access to cockpits via cyber means.

Last fall, reports emerged that a research team led by the DHS Science and Technology Directorate was able to remotely hack into the systems of a commercial passenger jet.

In the wrong hands, such a capability could result in mass casualties.

Even a much less drastic security breach could have major consequences.

The aviation sector relies on a vast network of interconnected systems, including air traffic control, airports, airline operations systems, and reservation and ticketing systems.

A cyber attack against any one of these systems could cause chaos and confusion, resulting in canceled flights and diminished consumer confidence.

Such an attack would likely cost airports and airlines millions and have lasting effects on the economy.

Despite the clear vulnerabilities and consequences of a cyber attack within the aviation sector, not much has been done to improve cybersecurity.

Although TSA requires airports and airlines to adopt and implement security programs covering a wide range of measures to protect against attack, TSA does not require those programs to include any cybersecurity measures.

Instead, TSA only shares a list of recommended best practices for airports and airlines to implement at their discretion.

When it comes to securing air travel, voluntary measures are not enough.

That is why I am working with my colleagues to develop legislation to require TSA to issue new rules for airports and airlines requiring implementation of baseline cybersecurity measures.

Additionally, while this hearing is focused on the aviation sector, I would be remiss if I did not note that these issues affect other modes of transportation as well.

Mass transit, passenger rail, freight rail, and pipeline systems all rely on networks that must be secured against cyber attacks.

It is my hope that today's hearing will provide us with more information on current cybersecurity efforts within the aviation sector and on what work remains to be done.

Again, I thank the witnesses for joining us, and I yield back the balance of my time.

Mr. RATCLIFFE. I thank the gentlelady. The Chair now recognizes the Chairman of the Subcommittee on Transportation Protective Security, the gentleman from New York, Mr. Katko, for his opening statement.

Mr. KATKO. Thank you, Chairman Ratcliffe. I am pleased our subcommittees could work together to hold this timely and obviously very important hearing.

In the wake of the devastating attacks on September 11, 2001, Congress created the Transportation Security Administration to protect and secure our Nation's transportation systems. Seventeen

years later, our aviation sector remains a highly attractive target for malicious actors who seek to inflict harm on the United States.

However, these threats have proliferated to include the realm of cybersecurity, something that was much less of a concern during the creation of TSA. The travel and tourism industries contribute trillions of dollars to the U.S. and global economy, and passenger volumes have steadily increased year after year. The fact that our aviation system is vital to the vibrancy and interconnectedness of our Nation is precisely what makes it such a highly-valued target.

Make no mistake about it: We are absolutely a highly-valued target by the bad guys, and they are constantly trying to probe how to get into systems and how to attack our airlines.

Protecting America's transportation systems is a collaborative effort between numerous Government and private-sector entities who share the goal of protecting the free movement of people and commerce. Therefore, as innovations in technology change the way our aviation sector operates, our collective security posture needs to adapt accordingly.

This hearing today will focus on cybersecurity in the aviation domain, and I look forward to discussing how TSA—and the Department of Homeland Security in general—interact with various stakeholders as partners to bolster the cybersecurity of the aviation ecosystem.

On any given day, the TSA and its partners in the aviation community secure around 2.4 million travelers, 1.2 million checked bags, and 8.4 million pounds of cargo. These security operations incorporate a wide array of technologies and invoke a considerable number of stakeholders, including airports, airline groups, and air carriers, among many others.

As the aviation community increasingly relies on connected systems for critical operations, we must acknowledge the urgency and importance of protecting the aviation sector's information technology systems and data against cyber threats.

The impact of cyber attacks can be far-reaching. In addition to significant security consequences, cyber attacks on the aviation sector can prompt considerable economic loss, passenger frustration, and undermine the public's trust in the aviation system.

As Chairman of the Subcommittee on Transportation and Protective Security, I have been a very vocal advocate for forward-leaning security policies and best practices to safeguard our Nation's transportation systems, and I believe we need to start thinking about cybersecurity as a critical element of that overall security posture.

That is why I am pleased to hold the hearing this morning with my colleagues from the Subcommittee on Cybersecurity and Infrastructure Protection. Our discussions surrounding aviation security should not ignore the vulnerabilities and risks posed by broad and interconnected systems with multiple vectors of attack.

As our systems in the air and on the ground become more advanced and more interconnected, cybersecurity will continue to be inextricably linked with aviation security.

TSA was created in the aftermath of 9/11 and charged with the mission of preventing another large-scale act of terrorism on American transportation system. While physical threats like improvised explosive devices continue to pose a major security concern, the re-

ality is that U.S. networks and databases are under daily cyber threat by nation-states, international crime organizations, and individual hackers.

Now, we need to pause for a second and really think about what this all means. Cyber threats can manifest themselves in many different ways. They can paralyze our systems or shut down the system. They could affect things such as SIDA access or access controls to secure areas, allowing people to get into secure areas who shouldn't be there. We know from recent incidents in Dallas-Fort Worth and elsewhere, enough criminal conduct goes on with people who have SIDA access. Imagine what could happen with people who don't and can get into those areas.

Airplane security, of course, is a big one. But let's not forget what was reported last year in 2017 where a report surfaced that Homeland Security was able to hack into a Boeing 757 that was sitting on the tarmac. Now, some people have harpooned various aspects of that report, but the specter remains that a plane could actually technically be weaponized against us and be taken over by bad guys through cybersecurity threats. That is something we need to talk about today and something we need to talk about tomorrow and all the way through.

As Ms. Watson Coleman alluded to, as well, same holds true for the transportation sector and trains, taking over a train and weaponizing a train. That is a new threat. It is a new frontier.

Our military has recognized this threat to such an extent that they have a Cyber Command. I am concerned that we may not be having the same priorities bestowed upon TSA and Homeland Security, and we have to understand the threat is real and it is going to keep getting worse.

This hearing illustrates my commitment to bringing a necessary focus to cybersecurity in the aviation sector, and I look forward to learning about the Federal Government's role in this space from our esteemed witnesses. I hope to understand how the partnerships between the Department of Homeland Security, TSA, and aviation stakeholders can be leveraged to make cyber risk awareness a key part of aviation security.

Thank you, Mr. Chairman. I yield back my time.

[The statement of Chairman Katko follows:]

STATEMENT OF CHAIRMAN JOHN KATKO

SEPTEMBER 6, 2018

Thank you, Chairman Ratcliffe. I am pleased our subcommittees could work together to hold this timely and important hearing. In the wake of the devastating attacks on September 11, 2001, Congress created the Transportation Security Administration to protect and secure our Nation's transportation systems. Seventeen years later, our aviation sector remains an attractive target for malicious actors who seek to inflict harm on the United States. However, threats have proliferated to include the realm of cybersecurity—something that was much less of a concern during the creation of TSA. The travel and tourism industries contribute trillions of dollars to the U.S. and global economy, and passenger volumes have steadily increased year after year. The fact that our aviation system is vital to the vibrancy and interconnectedness of our Nation is precisely what makes it such a highly-valued target.

Protecting America's transportation systems is a collaborative effort between numerous Government and private-sector entities who share the goal of protecting the free movement of people and commerce. Therefore, as innovations in technology change the way our aviation sector operates, our collective security posture needs to adapt accordingly. This hearing today will focus on cybersecurity in the aviation

domain, and I look forward to discussing how TSA—and the Department of Homeland Security in general—interact with various stakeholders as partners to bolster the cybersecurity of the aviation ecosystem.

On any given day, TSA and its partners in the aviation community secure around 2.4 million travelers, 1.2 million checked bags, and 8.4 million pounds of cargo. These security operations incorporate a wide array of technologies and involve a considerable number of stakeholders, including airports, airline groups, and air carriers, among many others. As the aviation community increasingly relies on connected systems for critical operations, we must acknowledge the urgency and importance of protecting the aviation sector's information technology systems and data against cyber threats. The impact of cyber attacks can be far-reaching. In addition to significant security consequences, cyber attacks on the aviation sector can prompt considerable economic losses, passenger frustration, and undermine the public's trust in the aviation system.

As Chairman of the Subcommittee on Transportation and Protective Security, I have been a vocal advocate for forward-leaning security policies and best practices to safeguard our Nation's transportation systems, and I believe we need to start thinking about cybersecurity as a critical element of that overall security posture. That is why I'm pleased to hold this joint hearing with my colleagues from the Subcommittee on Cybersecurity and Infrastructure Protection. Our discussions surrounding aviation security should not ignore the vulnerabilities and risks posed by broad and interconnected systems with multiple vectors of attack. As our systems in the air and on the ground become more advanced and more interconnected, cybersecurity will continue to be inextricably linked with aviation security.

TSA was created in the aftermath of 9/11 and charged with the mission of preventing another large-scale act of terrorism on the American transportation system. While physical threats like improvised explosive devices continue to pose a major security concern, the reality is that U.S. networks and databases are under daily cyber threat by nation-states, international crime organizations, and individual hackers. This hearing illustrates my commitment to bringing a necessary focus to cybersecurity in the aviation sector, and I look forward to learning about the Federal Government's role in this space from our esteemed witnesses. I hope to understand how the partnerships between the Department of Homeland Security, TSA, and aviation stakeholders can be leveraged to make cyber risk awareness a key part of aviation security.

Thank you, Mr. Chairman. I yield back.

Mr. RATCLIFFE. Thank the gentleman. Other Members of the committee are reminded that opening statements may be submitted for the record.

[The statements of Ranking Members Thompson and Richmond follow:]

STATEMENT OF RANKING MEMBER BENNIE G. THOMPSON

SEPTEMBER 6, 2018

Next week, we will observe the anniversary of the terrorist attacks of September 11, 2001.

Seventeen years ago, our adversaries exploited the cracks in our aviation security apparatus to carry out the deadliest terrorist attack in our Nation's history.

Since that time, we have focused on closing those gaps, making improvements to the way we share threat intelligence, screen passengers, and secure physical aviation infrastructure.

Although I recognize the progress we have made improving aviation security, I am concerned that we are overlooking an important attack vector: Cyber.

The aviation sector represents a wide array of critical assets, including the systems and networks that support airports, air traffic control, and aircraft, to name a few.

We rely on these diverse assets to support not only personal travel, but also commercial shipping, disaster relief, and a host of other activities essential to the health of our economy and National security.

All these assets are subject to a unique set of cybersecurity risks and vulnerabilities.

But we have done little to protect them against evolving cyber threats.

When it comes to physical security at our airports and our airplanes, we impose strict requirements designed to keep bad actors, explosives, and other illicit materials out.

But there are no equivalent cybersecurity standards.

Although we encourage owners and operators of aviation assets to take advantage of OHS cybersecurity programs and services, it is no substitute for requiring cybersecurity measures as part of site security plans.

And in many cases, aviation sector owners and operators struggle with the same cyber challenges that plague other industries: A National shortage of skilled cybersecurity personnel, a workforce with minimal cybersecurity training and awareness, and resource constraints across the board.

These gaps in our security framework represent "low-hanging fruit" for our adversaries.

A relatively simple intrusion could upend airport operations, costing airlines millions.

A more sophisticated breach of a cockpit could bring down a plane.

I am far from convinced that the Federal Government is investing enough in research around aviation-related cyber vulnerabilities.

Right now, some of the most significant Federal research in this area is being led by the OHS Science and Technology Directorate, which operates on a shoestring budget that Republicans in Congress continue to slash, year after year.

Nevertheless, last year, officials involved in this research reportedly managed to carry out a remote hack of a commercial passenger jet.

These findings underscore that this threat is real, and more attention is needed.

I look forward to hearing from this panel of witnesses today, and I hope they will give us a candid assessment of the cybersecurity posture of our aviation sector.

I will be interested to hear what progress has been made on areas like cyber threat information sharing, and how Congress can support those efforts.

STATEMENT OF RANKING MEMBER CEDRIC RICHMOND

SEPTEMBER 6, 2018

Seventeen years ago, 19 terrorists weaponized 4 passenger airplanes and launched the most devastating attack on U.S. soil since Pearl Harbor. As we struggled to understand how such a horrific tragedy could happen, the chairman of the 9/11 Commission issued a painful indictment: "This was a failure of policy, management, capability, and above all, a failure of imagination."

Since then, we have invested heavily in securing airplanes and airports against the kinds of attacks perpetrated by the 9/11 terrorists. But the threat landscape has evolved, and our adversaries have changed. Those who wish to do us harm have new tools at their disposal—giving them the ability to target aviation systems without stepping foot in an airport and without clear lines of attribution.

In March, the Department of Homeland Security and the FBI issued a joint alert warning that Russian government cyber activity had been targeting U.S. critical infrastructure, including the aviation sector. And research conducted by the DHS's Science and Technology Directorate have revealed troubling vulnerabilities in aircraft systems.

Although I am encouraged by Federal efforts to build awareness and address cybersecurity vulnerabilities to aviation infrastructure, I am concerned that we are, once again, playing catch up with our adversaries.

As we speak, the Transportation Security Administration does not require airport security plans to address cybersecurity vulnerabilities. It is unclear how cybersecurity factors into safety considerations involved in building aircraft. We must do better.

This hearing is an important step in our efforts to understand the full scope of cyber vulnerabilities to aviation assets and to help relevant Federal agencies work with stakeholders to manage and mitigate cyber risks. Pursuant to the National Aviation Security Strategy, an interagency task force—known as the Aviation Cyber Initiative—is charged with reducing cybersecurity risks to the Nation's Aviation Ecosystem.

The ACI is co-chaired by the Department of Homeland Security, the Department of Defense, and the Department of Transportation, and its charter is being updated to facilitate the tri-chair structure. I will be interested in hearing from our witnesses today about ACI's outreach to the stakeholder community and about the nature of aviation asset owners' and operators' engagement with the ACI.

More generally, I will be interested to learn how effectively the Federal Government shares cyber threat information across the aviation sector, and how that information informs efforts to harden assets, secure networks, and train aviation workers—from pilots and flight attendants to airport employees.

Finally, I will be interested in learning about the other challenges associated to improving the cybersecurity posture of the aviation industry—from technology to resources.

Mr. RATCLIFFE. We are pleased to have a very distinguished panel of witnesses before us today on this very important topic. Mr. Christopher Porter is the chief intelligence strategist for FireEye, as well as a senior fellow at the Atlantic Council. Previously, he had a distinguished 9-year career in the Central Intelligence Agency, working on cybersecurity issues.

Welcome, Mr. Porter.

Mr. Jeffrey Troy is the executive director of the Aviation Information-Sharing and Analysis Center and currently works as a senior IT manager at General Electric. Prior to this, Mr. Troy served for 25 years in the FBI, including his final stint as deputy assistant director of the cyber division.

We are grateful to have you here testifying today, Mr. Troy.

Finally, Mr. Michael Stephens is the executive vice president for IT and general counsel at the Tampa International Airport, where he has primary responsibility for all legal information technology, governance, regulatory, and compliance matters.

Welcome, Mr. Stephens. We are excited to hear your testimony, as well.

I would now ask the witnesses to please stand, if able, and raise your right hand so that I can swear you in to testify. Do each of you swear or affirm that the testimony which you will give today will be the truth, the whole truth, and nothing but the truth, so help you God? Let the record reflect that each of the witnesses has answered in the affirmative, and you may be seated.

The witnesses' full written statements will appear in the record. The Chair now recognizes Mr. Porter for 5 minutes for his opening statement.

STATEMENT OF CHRISTOPHER PORTER, CHIEF INTELLIGENCE STRATEGIST, FIRE EYE

Mr. PORTEIR. Thank you, Chairman Ratcliffe, Ranking Member Richmond, Chairman Katko, and Ranking Member Coleman, for convening this joint hearing today. We appreciate the opportunity to share FireEye's perspective on threats to the aviation sector and provide an overview of how we are helping to secure American aviation.

As was mentioned, my name is Christopher Porter. I am the chief intelligence strategist at FireEye. Our strategic intelligence products that inform my testimony today reach over 4,000 customers in 67 countries. Prior to joining FireEye, I worked at CIA for almost 9 years. That includes not only work with the agency, but also a short stint as the briefer at the White House for cyber threat intelligence issues, several years in counterterrorism operations, and war zone service, as well.

I want to share with you today FireEye's perspective, which is mostly informed responding to breaches in the aviation sector, but

also the intelligence that we have collected on what might be coming next to try to get ahead of the problem.

I am sure it will come as no surprise to the Members of these two subcommittees that the aviation sector is one of the most targeted for cyber attack that our company sees. Safe, reliable air transport is vital for everything from National defense to global commerce to personal freedom.

Malicious actors seeking to undermine America's strength in aviation through cyber attacks and through theft of data include foreign governments, terrorists, organized crime, and non-state actors acting on their own.

I want to start by discussing the most common cyber threat that the aviation industry faces, which is cyber espionage. Foreign governments routinely seek to steal industrial secrets from American manufacturers, researchers, designers, operators of military aircraft, and cutting-edge civilian planes. It is about who you would expect: China, Russia, more recently Iran have all targeted the United States or, in some cases, our close allies, who we share technology with overseas, to try and steal aviation secrets via computer network operations.

All three countries also routinely target ticketing and traveler data, shipping schedules and manifests, and partner industries, such as railways and hotels, mostly for domestic security reasons.

There are two aspects of cyber espionage, though, that I want to focus on. The first is that because it is a pervasive threat, the best defense against cyber espionage is rapid, detailed information sharing with context. Our company pushes alerts to customers in real time when possible. The technical alerts are in real time. We try to provide context within 24 to 48 hours.

Industry groups share information between peers, because as we have all learned, a threat to one is usually a threat to all. The U.S. Government also shares its threat information, although it is generally Classified and only available to cleared vendors. There is room for improvement at the speed of dissemination of intelligence, mostly from collector to agencies like DHS that then share it.

Most importantly, the timeliness of information within industry and between the private sector and the U.S. Government must improve, so it is not just the Government that has work to do.

The thing to know about cyber espionage, though, is that because it is routine, any one individual activity should not be viewed as destabilizing, you know, to the whole Nation. Media reporting on cyber incidents is naturally going to focus on the worst-case scenario of what could happen. Sometimes that is justified. Oftentimes it is not.

The public should not be needlessly alarmed or lose their confidence in what is, you know, generally a very safe industry because of individual cyber espionage incidents. Every major cyber power, including the United States, has an interest in knowing about the potential defense technology developments of both its friends and potential threats, and the U.S. aviation sector isn't the only one that is being targeted in this way.

So while espionage on its own does not pose an urgent threat to life, I am concerned that continued theft or trade secrets could pose a long-term threat to American economic health. Aviation is one of

our Nation's leading export industries. China in particular is harnessing all aspects of national power to displace the United States as a military and economic power.

Chinese theft of intellectual property for commercial purposes has almost entirely dropped off since the September 2015 agreement between President Xi of China and President Obama. You know, diplomacy does work as a cybersecurity means.

However, that depends a lot on what industry you are in. For the aviation security, research and development is so closely tied to National defense that it really never stopped being targeted. So, you know, unfortunately, the matter before these committees is not defended by those diplomatic efforts. They continue.

Cyber criminals, likewise, pose an economic threat to the aviation sector and its customers. For years, we have seen airlines and third-party ticket sellers exploited so that illicit tickets could be resold for profit in underground fora. In the last 2 years, our devices have detected a sharp increase in the use of ransomware to temporarily disable airline ticketing and support operations. That is often untargeted, not specifically aimed at airports, but as we have seen, it could be, as well.

Air travel is a time-sensitive business. Cyber criminals know they can extort payment from airline that are unable to move passengers until their systems are decrypted.

Finally, in addition to threats to the aviation sector's proprietary information customer records and systems that support flight operations, there are cyber threats that are intended to use aviation's prominent place in our lives as a means of creating psychological damage when it is effected.

Airports in Europe, the Middle East, Southeast Asia, to a limited extent here at home have had their websites defaced or disrupted in order to draw attention to political causes. The primary victim in those situations are members of the public who may wrongly fear that a loved one is at risk or grow in their distrust of flying, even though the affected systems are public relations-focused or don't support flight operations.

So it is important that officials and airline representatives communicating with the public during such events differentiate between systems that are affected, where if you take them down it just causes inconvenience or reputational damage, versus systems that if they are targeted or damaged, you know, directly support flight operations and could affect passenger safety.

So thank you again for the opportunity to participate in today's discussion. I thank you for your leadership improving cybersecurity in the aviation sector. I look forward to working with you to strengthen our partnership, and I am happy to answer any questions from the committee.

[The prepared statement of Mr. Porter follows:]

PREPARED STATEMENT OF CHRISTOPHER PORTER

SEPTEMBER 6, 2018

Thank you Chairman Ratcliffe, Ranking Member Richmond, Chairman Katko, and Ranking Member Coleman for convening this joint hearing today. We appreciate the opportunity to share FireEye's perspective on threats to the aviation sector and provide an overview of how the private sector is helping to secure the sector.

My name is Christopher Porter, and I'm the chief intelligence strategist for cybersecurity company FireEye and a nonresident senior fellow at the Atlantic Council. At FireEye I manage our "Intelligence for Executives" program for senior corporate and government clients across the globe. Our strategic intelligence products reach more than 4,000 customers in 67 countries.

Prior to joining FireEye in 2016, I served for nearly 9 years at the Central Intelligence Agency, including an assignment as the cyber threat intelligence briefer to White House National Security Council staff, several years in counterterrorism operations, and warzone service.

In addition to the 300-plus security professionals responding to computer intrusions, FireEye has over 200 cyber-threat analysts on staff in 18 countries, speaking 30 different languages, to help us predict threats and better understand the adversary—often by considering the political and cultural environment of the threat actors. We have an enormous catalog of threat intelligence, and it continues to grow everyday alongside the continually increasing attacks on organizations around the world.

FireEye is supporting the aviation sector here at home. We're protecting the Transportation Security Administration with both email and web inspection, managed by the Department of Homeland Security's Enterprise Security Operations Center. As TSA continues to stand up its intelligence capabilities, we are providing support through their subscription to our intelligence reporting.

The Federal Aviation Administration also makes great use of our intelligence reporting and they're using our malware analysis tool to help prevent and detect future cyber attacks.

I want to share with you today FireEye's perspective responding to breaches in the aviation sector and from the intelligence we have collected on what might be coming next.

I am sure it will come as no surprise to you that the aviation sector is one of the most targeted for cyber attack. Safe, reliable air transport is vital for everything from National defense to global commerce to personal freedom. Malicious actors seeking to undermine America's strength in aviation through cyber attacks and theft include foreign governments, terrorists, organized crime, and other non-state actors.

I want to start by discussing the most common cyber threat facing the aviation industry: Cyber espionage. Foreign governments routinely seek to steal industrial secrets from manufacturers, researchers, designers, and operators of both military aircraft and cutting-edge civilian planes. China, Russia, and more recently Iran have all targeted the United States or its close allies for theft of aviation secrets via computer network operations.

All three countries also routinely target ticketing and traveler data, shipping schedules and manifests, and partner industries such as railways and hotels as they gather counterintelligence data on suspicious travelers and intelligence on VIPs they wish to track.

There are two aspects of cyber espionage targeting the aviation sector overall that I want to emphasize: First, that because of its pervasive nature, the best defense against cyber espionage is rapid, detailed information sharing with context. Our company pushes alerts to customers in real time, and industry groups share information between peers because, as we have learned, a threat to one is often a threat to all. The U.S. Government also shares threat information, although it is generally Classified and available only to cleared vendors; there is room for improvement in Government information sharing with uncleared industry partners. Most importantly, the timeliness of information within industry and between the private sector and U.S. Government must improve. In my line of work, if we can't provide context and additional information in 24–48 hours of an attack, we have not met customer expectations.

The second thing to know about cyber espionage though is that, because it is routine, it should not be viewed as destabilizing. Media reporting on cyber incidents is often focused on the worst-case scenario in ways that are sometimes unjustified and needlessly alarm the public or inflame opinion against a foreign adversary. Every major cyber power, including the United States, has an interest in knowing about the potential defense technology developments of both its friends and potential threats, and the U.S. aviation sector is not unique in being targeted in this way.

When cyber espionage operators get a foothold on a system, they can often use that access for stealing information or to launch a disabling or destructive attack using the same technology. But they rarely choose to do so, and in the United States there are significant redundancies in place to ensure safety. A crashed IT system does not mean a crashed plane, and it's important for the public to keep that in mind.

So while cyber espionage on its own does not pose an urgent threat to life, I am concerned that continued theft of trade secrets poses a long-term threat to American economic health. Aviation is one of our Nation's leading export industries, and China in particular is harnessing all aspects of National power to displace the United States as a military and economic power in Asia and world-wide. Chinese theft of U.S. intellectual property for commercial purposes has almost entirely dropped off since a September 2015 agreement between President Xi of China and President Obama, but because aviation research and development is so closely tied to National defense this particular sector of the American economy never stopped being targeted.

Chinese hackers pursue fewer targets in the United States than they did before the Xi-Obama Agreement, but they have just as many hackers who are more skilled and better resourced than ever, meaning that industries that do continue to be threatened face a greater threat than ever before that technologies the United States spends billions developing will be stolen and adopted by economic competitors and military rivals in China.

Cyber criminals likewise pose an economic threat to the aviation sector and its customers. For years we have seen airlines and third-party ticket sellers exploited so that illicit tickets could be resold for profit in underground fora. Because airlines are trusted by their customers with a wide variety of sensitive personal data, they are also frequently targeted by cyber criminals looking to gather data to enable other types of fraud. In the last 2 years, our devices have detected a sharp increase in the use of ransomware to temporarily disable airline ticketing and support operations—air travel is a time-sensitive business, and cyber criminals know that they can extort quick payment from airlines that are unable to move passengers until their systems are decrypted.

Finally, in addition to threats to the aviation sector's proprietary information, customer records, and systems that support flight operations, there are cyber threats intended to use aviation's prominent place in our lives as a means of creating psychological damage or political pressure. Airports in Europe, the Middle East, Southeast Asia, and here at home have had their websites defaced or disrupted, mostly by non-state actors seeking to draw attention to a particular political cause.

The primary victim in these situations are members of the public who may wrongly fear that a loved one is at risk or grow in their distrust of flying, even though the affected systems may be public relations-focused and support no flight operations at all. The fear these operations cause is particularly pronounced when those outages are caused by groups affiliated with terrorists.

In other cases, these virtual sit-ins that affect a company's website have, in limited cases, delayed takeoffs for airlines that also relied on those computers to make or distribute flight plans, though even these attacks did not have a direct effect on flight safety.

It is important that officials and airlines representatives communicating with the public during such events differentiate between taking down systems that cause inconvenience from those that directly support flight operations and passenger safety.

CONCLUSION

Thank you again for the opportunity to participate in today's discussion. Thank you for your leadership improving cybersecurity in the aviation sector. I look forward to working with you to strengthen the partnership between the public and private sectors and to share best practices to thwart future cyber attacks. I'm happy to answer any questions from the committee.

Mr. RATCLIFFE. Thank you, Mr. Porter.

The Chair now recognizes Mr. Troy for his opening statement.

STATEMENT OF JEFFREY L. TROY, EXECUTIVE DIRECTOR, AVIATION INFORMATION-SHARING AND ANALYSIS CENTER

Mr. TROY. Good morning. My name is Jeffrey Troy. I am the executive director of the Aviation Information-Sharing and Analysis Center. The Aviation ISAC is a global, member-driven, nonprofit company. Our member companies are headquartered on five continents and represent a cross-section of the many businesses that make up the aviation ecosystem.

They include the makers of aircrafts, their engines, airlines, airports, satellite communication providers and aviation services, as

well as their supply chains. The mission of the Aviation ISAC is to increase the cyber resiliency of the aviation sector across the world.

Safety comes first in every aspect of the aviation industry. Cybersecurity is no exception. Each segment of our industry has numerous automated computer-based processes which contribute to the overall safety and efficiency of aviation. Each member of the Aviation ISAC has a chief information security officer or someone comparable who assumes the responsibility of protecting the computer networks and products that are performing the operations of the business and protecting them from cyber attack.

The Aviation ISAC works with each CISO to understand their company's risk profile. We use this information to drive industry programs and to reduce cyber risk. The Aviation ISAC builds communities of experts within each of the specialties supporting the CISO. These include cyber threat analysts, compliance experts, network security architectures, and product security specialists.

Each community leverages the combined capabilities of members to expedite the development of solutions and intelligence to either reduce or eliminate risk. We facilitate automated and in-person intelligence exchange training, best practices, and tabletop exercises. We proactively hunt for treats, stolen network access, indicators of compromise, and we engage with security researchers.

Our focus is on finding information that can be used by the aviation industry to reduce cyber risk and increase operational resilience. Every business and every industry, including aviation, can only succeed when the needs and the concerns of the customers are met. This includes addressing misperceptions.

Flying is the safest mode of transportation. However, there have been times over the past few years when persons incorrectly allege they were able to impact the safety of flight by hacking a system on a plane.

The Aviation ISAC has addressed these issues head on. Working with industry and coordinating with Government partners, we play a leading role in investigating alleged vulnerabilities and conducting extensive testing to ferret out any vulnerabilities, validated or invalidated.

The Aviation ISAC recognizes the value of the work of cybersecurity researchers in finding these vulnerabilities, even if the vulnerabilities are minor, contained, and do not pose a risk to flight safety. The aviation industry will continue to investigate vulnerability claims and take swift action when required. As of today, none of the vulnerabilities that have been investigated by the Aviation ISAC or its members have impacted the safety of flight.

The Aviation ISAC is also pleased to have a strong and productive relationship with our Government partners. Indeed, liaison with Government was part of the founding idea of the Aviation ISAC. We collaborate in many forms and on a wide scope of aviation, cybersecurity-related projects.

For example, in a recent engagement with a threat researcher who sensationalized the claim of being able to hack a plane, we kept both our industry members and Government partners well-apprised of our work to include the sharing of technical details. We engaged with the Department of Homeland Security, Transpor-

tation Security Administration, the Federal Aviation Administration, and the European Aviation Safety Agency.

The aviation industry, like all industries with all extensive digital integration, has not declared victory, but rather is constantly engaged in the battle. As I said earlier, in aviation, security and safety comes first. Digital enhancements to processes are adopted at a deliberate pace to ensure that there is no impact to safety. Security around the digital processes begins in the design stages and runs through the build, deploy, operate, and continuously monitor phases.

Air framers and their suppliers extensively test new technologies and design layered safety and security controls, both digital and physical, to ensure the highest level of safety in flight.

We do not know what we do not know. Many vulnerabilities in computer systems were discovered years after the systems were designed and deployed. New technologies are being added to existing platforms. As such, as our industry is constantly red-teaming our systems and seeking to uncover issues before they become impactful.

We believe safety and security are significantly enhanced when companies and Government agencies communicate on cyber threats and vulnerabilities. On behalf of all of our members, I thank you for the opportunity to come before you today and answer questions about cybersecurity and cyber resilience in the aviation industry.

[The prepared statement of Mr. Troy follows:]

PREPARED STATEMENT OF JEFFREY L. TROY

SEPTEMBER 6, 2018

Good morning. My name is Jeffrey Troy. I am the executive director of the Aviation Information-Sharing and Analysis Center. The Aviation ISAC is a global, member-driven, non-profit corporation. Our member companies are headquartered on 5 continents and represent a cross-section of the many businesses making up the aviation industry ecosystem. They include the makers of aircraft, engines, airlines, airports, air traffic control, ground traffic control, satellite communication providers, and aviation services as well as their supply chains. The mission of the Aviation ISAC is to increase the cyber resiliency in aviation world-wide.

Safety comes first in every aspect of the aviation industry, and cybersecurity is no exception.

Each segment of our industry has numerous automated, computer-based processes, which contribute to the overall safety and efficiency of aviation. Each member of the Aviation ISAC has a chief information security officer (CISO) or someone comparable who assumes the responsibility of protecting computer networks and products performing the operations of the business from cyber attacks. The Aviation ISAC works with each CISO to understand their company's risk profile. We use this information to drive industry cooperation and collaboration on projects and programs to reduce cyber risk.

The Aviation ISAC builds communities of experts within each of the specialties supporting the CISO. These include cyber threat analysts, compliance experts, network security architects, and product security specialists. Each community leverages the combined experience and intelligence capabilities of the members to expedite the development of solutions and intelligence to reduce or eliminate risk.

We facilitate automated and in-person intelligence exchange, training, best practices, and table-top exercises. We proactively hunt for threats, stolen network access, indicators of compromise, and engage with threat researchers. Our focus is on finding information that can be used by the aviation industry to reduce cyber risk and increase operational resilience.

Every business and every industry, including aviation, can only succeed when the needs and concerns of their customers are met. This includes addressing misperceptions. Flying is the safest mode of transportation. However, there have

been times over the past few years when persons incorrectly alleged they were able to impact flight safety by hacking a system on a plane.

The Aviation ISAC has addressed these issues head-on. Working with industry and coordinating with Government partners, we play a leading role in investigating alleged vulnerabilities, and conducting extensive testing to ferret out any vulnerabilities validated or invalidated. The Aviation ISAC recognizes the value of the work of cybersecurity researchers in finding cyber vulnerabilities, even if those vulnerabilities are minor, contained, and do not pose a risk to safety. The aviation industry will continue to investigate vulnerability claims and take swift action when required. As of today, none of the vulnerabilities that have been investigated by the Aviation ISAC or its members have impacted the safety of flight.

The Aviation ISAC also is pleased to have a strong and productive relationship with our Government partners. Indeed, liaison with Government was a founding idea behind the creation of the ISAC. We collaborate in many forums and on a wide scope of aviation, cybersecurity-related projects. For example, in a recent engagement with a threat researcher who sensationalized a claim of being able to "hack a plane," we kept both our industry members and Government partners well-apprised of our work to include the sharing of technical details. We engaged with the Department of Homeland Security, Transportation Security Administration, the Federal Aviation Administration, and the European Aviation Safety Agency.

The aviation industry, like all industries with extensive digital integration, has not declared victory, but rather is constantly engaged in the battle.

As I said earlier, in aviation, safety comes first. Digital enhancements to processes are adopted at a deliberate pace to ensure no impact to safety. Security around the digital processes begins in the design stages and runs through the build, deploy, operate, and continuously monitor phases. Airframers and their suppliers extensively test new technologies and design layered safety and security controls, both digital and physical, to ensure the highest level of assurance in flight safety.

We do not know what we do not know. Many vulnerabilities in computer systems were discovered years after the systems were designed and deployed. And new technologies are being added to existing platforms. As such, our industry is constantly red-teaming their systems and seeking to uncover issues before they become impactful.

We believe safety and security are significantly enhanced when companies and Government agencies communicate on cyber threats and vulnerabilities. On behalf of all our members, I thank you for the opportunity to come before you today and answer your questions about cybersecurity and cyber resilience in the aviation industry.

Mr. RATCLIFFE. Thank you, Mr. Troy.

The Chair now recognizes Mr. Stephens for 5 minutes for his opening statement.

STATEMENT OF MICHAEL A. STEPHENS, EXECUTIVE VICE PRESIDENT, IT AND GENERAL COUNSEL, TAMPA INTERNATIONAL AIRPORT

Mr. STEPHENS. Thank you, Mr. Chairman. Chairman Ratcliffe, Chairman Katko, Ranking Member Richmond, Ranking Member Watson Coleman, and Members of the subcommittee, good morning. My name is Michael Stephens. I am the executive vice president and general counsel for information technology for Tampa International Airport. We thank you for the opportunity to participate in today's hearing on the critically important topic of understanding and mitigating cybersecurity threats to our Nation's airlines, airports, and our critical aviation infrastructure.

More than 2.5 million passengers travel safely in and out of America's airports each and every day. The largest 5 U.S. airports alone move more passengers through them on an annual basis than the entire population of the United States. Our airports facilitated the shipment of more than 40 billion pounds of cargo. In total, the aviation sector contributes approximately 5.1 percent to our National GDP.

Aviation is essential, not only to our economic prosperity, but to our National security interests, as well. In order to meet the increasing demand of the needs of international commerce and the traveling public, virtually all of the essential airport operations and functions, as well as aviation safety, security, access control, navigations, communications, industrial systems controls, and emergency response systems must rely heavily on a multitude of technology applications and platforms.

For that reason, it is my opinion, like the other witnesses here, that cybersecurity risks without question represent the most preeminent and persistent threat to the continuous safe, secure, and efficient operations of U.S. airports in the global aviation system.

Airports and airlines defend against hundreds of thousands of malicious intrusion attempts each and every day. In short, computers, kiosks, and keyboards have become the newest tools of criminals and the new weapons of war. It is of paramount importance that we exercise increased urgency and vigilance to mitigate cybersecurity threats to our Nation's critical aviation infrastructure.

While there is no silver bullet or perfect defense against cybersecurity threats within the aviation industry, there are some critical areas that I believe present great opportunities for airports, along with our airline partners and aviation stakeholders to achieve greater preparedness, responsiveness, and resilience.

First, the adoption of a standard. Although airports and airlines and other aviation stakeholders have engaged in building and achieving the levels of cybersecurity capability, maturity, and resilience, there are currently no minimum standards or frameworks being used across the sector. In fact, according to a survey of U.S. airports by the Airport Cooperative Research Program and its guidebook on best practices for airport cybersecurity, only 9 out of 24, or 34 percent, of airport respondents indicated that they had implemented a National cybersecurity standard or framework.

I believe significant considerations should be given by airports and airlines to mandate within their respective organizations the adoption and implementation of established cybersecurity standards and frameworks.

A second opportunity is what the witnesses who are joining me here today have talked about, and that is the increased sharing of information and threat intelligence, because it is a critical component for airports to assess our vulnerabilities and to enhance our preparedness and more effectively respond and recover in the event of a critical cyber incident.

It is essential to have strength in information sharing, and consideration should be given to more proactive and broader disclosure within the sector by airports and airlines of cybersecurity incidents that meet an agreed-upon threshold, irrespective of whether or not the incident resulted in a data breach or a system compromise.

Finally, the human factor. The human factor remains the most highly-exploited vector for penetrating cybersecurity defenses. Cybersecurity threat awareness and information security training programs for all airports, airline, and aviation sector employees is perhaps the most effective and cost-efficient way of increasing airport and airline cybersecurity readiness.

Airports and airlines should be given strong consideration to adopting uniform standards which establish baseline training requirements for airport, airline, and other key aviation sectors' employees on a defined and reoccurring basis.

As the adoption of current and future technologies increases to support the aviation sector, the threat of disruptive cyber attacks on airports, airlines, and critical aviation information sector systems undoubtedly will increase, as well. Evolution toward a more effective cyber risk management mitigation strategy by airports, key aviation sector stakeholders, through the adoption and implementation of baseline cybersecurity frameworks and standards is absolutely essential to the Nation's security and long-term prosperity.

Again, I thank you for the opportunity to testify before you all today, and I look forward to answering any questions that you may have.

[The prepared statement of Mr. Stephens follows:]

PREPARED STATEMENT OF MICHAEL A. STEPHENS

SEPTEMBER 6, 2018

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

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

The size and scope of operations, as well as the passenger volume in our Nation's airports is vast. The FAA classifies the Nation's 30 largest airports by passenger volume, as large hub airports. Tampa International is in that category. Out of those 30 airports designated as large hubs, the top 4 or 5 have more passengers flowing through them on an annual basis than the entire population of the United States.

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

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

The operational importance of these systems coupled with the fact that they are often interconnected through networks and remote access points makes airports, immensely appealing targets and potentially vulnerable to malicious cyber threats, such as criminal organizations and state-sponsored actors.

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

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

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

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

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

While there is no perfect defense against cybersecurity threats within the aviation industry or any industry for that matter, there are critical activities that we must undertake to mitigate as many risks as possible. For the purposes of this hearing, I have distilled my remarks down to three critical areas that I believe present the best opportunity for airports along with our airline partners and aviation sector stakeholders to achieve greater preparedness, responsiveness, and resilience.

MANDATORY MINIMUM STANDARDS

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

Although, airports, airlines, and other aviation stakeholders have engaged in building and achieving various levels of cybersecurity capability, maturity, and resilience, there are currently no significant requirements for adherence to minimum standards for preparedness. According to a survey of airports in the United States, by the Airport Cooperative Research Program (ACRP) as published in 2015 in its Guidebook on Best Practices for Airport Cybersecurity, only 9 out of 24 (34 percent)

of airport respondents indicated that they had implemented a National cybersecurity standard or framework.

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

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

CYBERSECURITY INFORMATION SHARING & COMMUNICATION

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

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

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

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

INFORMATION SECURITY AWARENESS AND WORKFORCE TRAINING

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

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

Numerous resources are available for cybersecurity training at the Federal, department, and State level. According to the survey of airports in the United States, by the Airport Cooperative Research Program (ACRP) as published in 2015, 20 of 27 (74 percent) of the responding airports indicated that they engage in some form of employee information security awareness training. However, due to the multitude of differences within airport governance and organizational structures, the scope, depth, and quality of training may vary significantly from airport to airport. Numerous additional factors may also adversely impact the quality and scope of training

such as availability of budgets, subject-matter expertise and adequate buy-in from senior management. Adopting and requiring a uniform standard which establishes a minimum training requirement for airport, airlines, and other aviation-sector employees on a defined and reoccurring basis should be given strong consideration by Congress and appropriate aviation sector regulatory agencies such as the FAA and TSA.

CONCLUSION

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

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

Mr. RATCLIFFE. Thank you, Mr. Stephens. We will now move into the questioning portion of our hearing. I will recognize myself for 5 minutes.

Mr. Porter, I want to start with you. FireEye has been very vocal about APT33 and its links to the Iranian government. APT33 has targeted, among other things, Middle Eastern carriers and airports and utilities. So I want your perspective on how Iran is using cybersecurity as a geopolitical tool. More specifically, how does—if you can get into how breaching the airlines and airports of its neighboring countries furthers the geopolitical goals of the Iranian regime?

Mr. PORTER. Sure, thank you, Mr. Chairman. The perspective that I have on what Iran and all the other major antagonists of the United States and its allies, they basically are all engaged in the same class of activity, which is, for the most part, they are looking at domestic security, so, you know, looking at traveler movements and that sort of thing.

So for them, it is probably viewed mostly as a domestic security issue, looking at what is going on in the region. It is, however, also an opportunity for them to look at what the United States is doing with its partners, intelligence gathering in support of military operations or in support of their own technological and economic development.

So I think for them they would view it as it naturally being in their backyard to look at this from a security perspective, not necessarily—as I mentioned in my opening remarks, not necessarily an attack.

The thing to keep in mind, Mr. Chairman, is that any foothold that any adversary gets into a system that is used for cyber espionage, which is widespread and everyone does it, that can easily be turned into an attack. That same foothold can be used and turned, depending on the willingness of the aggressor as an attack vector. By attack, I mean disabling the computer system, not necessarily causing kinetic action against an airplane.

But the primary restraint is not technological. It is going to be the willingness of the actor to do that.

Mr. RATCLIFFE. Perfect. I want to ask you a little more broad question, as—you know, innovation in technology widens the attack surface. I am wondering how FireEye is spending its time these days, in terms of what is the most frequent, most likely venue of attack with respect to the aviation sector?

Mr. PORTER. Sure. Thank you for that question, Mr. Chairman. If I were looking at it from an adversary's perspective, I think the real weakness of the aviation sector isn't going to be something like the airplanes themselves, which have a lot of resilience, and the class of actors that could bake in a destructive capability against an airplane by cyber means also have other means of disabling airplanes.

So what I am primarily concerned about is reputational damage. Could you go out and make people think that airplanes are unsafe? Could you hack websites and then create the perception that it is no longer safe in a region? That could cause massive economic damage that a CISO sitting at an airport or an airline or a manufacturer would have a hard time defending themselves against, because they are not really the direct target. It is the system of interconnected computers, some of which may not even be under their physical control. It could be a third-party system that is compromised and used to draw attention to what—you know, alleged safety deficiencies.

I would also say, secondarily, I am concerned that some actors are that capable of causing kinetic loss of airplanes through traditional, conventional means might claim that downing an airplane was the result of a hacker, in other words, there is no actual cyber threat, but the feasibility of it could be used to explain a loss by other means. So I think you could see that coming, as well.

That is why it is important to keep the public, I think, just the right amount of scared, you know, enough to want to invest in defense and resilience, especially, but not necessarily assuming that every case of cyber espionage is leading to an attack. Because that is another way of interpreting my remarks, is that if cyber espionage is pervasive and there is no attacks happening, that will imply that the willingness to do so isn't there at this time. People should keep that in mind, as well.

Mr. RATCLIFFE. I want to move to you, Mr. Troy. The transportation sector—and of course, within that, the aviation industry has two sector-specific agencies that they have to work with in the Department of Transportation and the Department of Homeland Security. As I referenced in my opening statement, TSA, NPPD, FAA, they all have equities in this space.

I want your perspective from the ISAC perspective, I guess, with regard to what I mentioned in terms of how well those entities are sort-of playing with one another in that space and whether or not there needs to be greater clarity with respect to the roles or issues that we need to be aware of in addressing.

Mr. TROY. So the Aviation ISAC, we have a lot of touchpoints with each of those agencies. When the Government set up each of the 16 critical infrastructure sectors, they created the Government coordinating committees and on the industrial side the sector coordinating committees for each of the sectors.

So the Aviation ISAC is a part of the aviation sector coordinating committee. Through that, we meet regularly with each of those different agencies and work on the highest-priority projects for protecting the sector.

Separately, we have a person that is on the floor of the NCICC inside of NPPD. We have a person who is daily at the ADIAC, the Air Domain Intelligence Analysis Cell, which is run by the TSA, and we have routine engagement with the FAA.

So I would characterize each agency as very much understanding what their different roles are and through those and other forms that they are protecting—working well in terms of efforts to protect the sector.

I would like to also recognize that NPD's movement toward this risk management center I think is a very good move to see, because I think risk management frameworks, which were mentioned also by Mr. Stephens, are a critical part of the process in terms of maturing the cybersecurity capability of each of the segments inside the industry.

Mr. RATCLIFFE. Thank you. My time has expired.

I recognize the gentlelady from New Jersey, Mrs. Watson Coleman.

Mrs. WATSON COLEMAN. Thank you, Mr. Chairman, and thank you to each of you for the information you have shared with us today.

Mr. Stephens, I want to start with you. You represent an airport. Are airports currently required to include any cybersecurity measures in their plans?

Mr. STEPHENS. Congresswoman Watson Coleman, thank you for that question. At this time, there is no absolute requirement to do so. The governing regulations 14—excuse me, 49 CFR part 1540, which is administered primarily by the TSA, has primarily been focused on physical security, access to the sterile air site areas, making sure SIDA badges are checked, all of those types of things.

But as all of you have pointed out correctly, the cybersecurity element has penetrated the domain of the physical security element, and yet that similar type of posture hasn't been moved over to address the baseline standard on the cybersecurity side for airports.

Mrs. WATSON COLEMAN. Thank you. So if you are not aware, though, pretty sure that you in general, and Mr. Porter and Mr. Troy, aren't aware of any required standards, either?

Mr. TROY. No, I am not.

Mrs. WATSON COLEMAN. Thank you. Mr. Stephens, you indicated three things that I thought were really important—the adoption of standards, the increased sharing of information and threat analysis, and the human factor of baseline training.

Mr. STEPHENS. Yes, ma'am.

Mrs. WATSON COLEMAN. What do you believe is the role of the DHS and the TSA in each of those things? Is this a matter of additional resources or prioritization?

Mr. STEPHENS. Well, again, that is a great question. Resources are always an issue, but I think that prioritization is one of the critical areas that we have to focus on. Again, there are fantastic standards out there. DHS and the Federal Government imple-

menting the NIST standard is an excellent standard out there, except that there hasn't been broad and widespread use of those standards in the aviation sector, particularly with respect to airports.

DHS, for example, offers cybersecurity and WiFi testing. We have used and taken advantage of it at Tampa International. It has been a great tool. So there are tools out there. I think there has to be a more aggressive posture with airports and the airline industry in actually leveraging and using those tools.

Yes, that may be a function of resources. I know DHS is tasked heavily just trying to implement the requirements of the statute on the Federal side, so there is an issue there. But then second, the training element is important. I do believe that there may be some room for at least having airports adopt a baseline standard.

Again, as we like to say in our industry, you have seen one airport, you have seen one airport, because they are governed very differently, their structures are set up very differently. But having the notion of a baseline cybersecurity standard I think goes a long way.

Mrs. WATSON COLEMAN. So, gentlemen, I am very concerned about land transportation, train stations, freight, you know, all those things, buses. Do you believe that what we could develop to be more proactive and represent greater protection on cybersecurity threats in the aviation industry can also be applied to ground transportation systems?

Mr. STEPHENS. You know, I would like to maybe start on that, because before I became the general counsel and CIO for the aviation authority, I was with surface transportation, our equivalent of DC Metro. The exact same risks are out there, when you look at things like automated train control, when you look at signalization, when you look at signalization and priority at all of our crossing points.

So the exact same risks exist. I think the difference to a certain extent—and this may be anecdotal—there is a more pervasive feeling from the—you know, the traveling public when you think about catastrophic attacks or disruptions in airports. I mean, if you look at Atlanta, what happened with a fire incident that was not related to cybersecurity, you are talking about passengers being stranded on airplanes and in terminals for hours, $40 million worth of direct value lost. But the exact same threats exist on the surface transportation side, absolutely.

Mrs. WATSON COLEMAN. Thank you. Mr. Troy, Mr. Porter, you might have a comment on that?

Mr. TROY. I would agree with that statement that there are systems that are—have common functions in terms of helping to move the industry. As we move toward smart cities and more and more of the controls, again, are automated, they run that risk that those industrial security control tools, which are common across the industries, could be under attack.

Mrs. WATSON COLEMAN. Thank you.

Mr. PORTER. Yes. Leaving aside discussion of the attack surface, the shared technology I think, the same sort of adversaries that would be interested in disrupting one would be interested in disrupting the other. We do see that they use the same infrastructure to attack both. So information sharing would help both.

Particularly for—I think for military logistics, for example, you have got a long train—no pun intended—between the United States and wherever soldiers are deploying and for their equipment. It is going to go over a variety of methods, individual mom-and-pop trucking companies, trains, you know, air freight, and it may eventually end up in a naval port loading onto a Navy ship.

So if you can disrupt any one of those, even if it is civilian-owned and -controlled, you can, you know, disrupt a deployment ability. So certainly I would agree that it is valuable to pursue.

Mrs. WATSON COLEMAN. Thank you, gentlemen. I yield back, Mr. Chairman.

Mr. RATCLIFFE. Thank the gentlelady. The Chair recognizes the gentleman from New York, Chairman Katko, for 5 minutes.

Mr. KATKO. Thank you, Mr. Chairman. I appreciate all of your testimony here today. I just want to circle back for a moment back to my opening statement, and some of the things I noted in there about how systems could be paralyzed and the concern with SIDA access, as well as airplane and rail security itself.

Mr. Porter, you kind-of alluded to that. You didn't think it is as likely to have an attack on—a cyber attack on a rail or airplane that could basically weaponize it. Is that accurately portraying what you said?

Mr. PORTER. You know, I don't want to get too much into specifics and mislead you about my expertise. I can't—I would defer, I think, to the DHS study on the feasibility. I just think it is much more likely that the reputational damage scenarios are much more likely to occur.

However, I did note in your opening remarks and I certainly would agree, Mr. Chairman, that the sort of nightmare scenarios where a plane or something like that is weaponized probably involves someone getting physical access. I think that opens up a whole different world of opportunities for cyber attack.

So to minimize the chance of that happening, certainly physical controls are going to be, arguably, from my perspective, one of the most important ways of addressing that particular concern. As others on the panel have pointed out, you never know what you don't know, and a dedicated adversary could, of course, research a very specific vulnerability, but even then it might require physical access. I think that is a great thing for us to focus on defensively.

Mr. KATKO. Yes, and that kind-of gets to my point. These threats are real. I mean, we are talking about things kind-of at the 30,000-foot level, but let's face it. I mean, the threats we have, since I have been a Congressman, I have had my stuff hacked. Somebody tried to open up accounts for me in my name on the West Coast, bank accounts. That was a direct result of my Government records being hacked.

So I don't think there is many people in this room who haven't had some sort of a cyber attack perpetrated upon them. So to think of the vulnerabilities that are at these airports and the ones I spoke about, to name a few, and the access controls is a huge issue for me, too. Then to hear what Mr. Stephens said, which was shocking to me, was that on a survey of the 24 airports, whatever it was, less than a third said they have implemented any sort of cybersecurity strategy, that is in line with what you are thinking.

That is frightening to me. That is absolutely ridiculous that we countenance that.

So to all of you, I want to hear what you think we should be doing to address that.

Mr. STEPHENS. Mr. Chairman, I think one of the first areas is a greater insistence and urgency that maybe just falls very short of the notion of wholesale regulation, but to make sure that airports when we do our security checks, when TSA comes to check under their governing provisions and when FAA checks for airfield security, that there is some consideration of checking to see if an airport at least has a basic cybersecurity protocol in place to identify, react, respond——

Mr. KATKO. May I interrupt? I am sorry to interrupt you, but I am short on time and I did want to make sure I get to this. Do I understand you correctly, when they come and do airport assessments, they don't assess the cyber vulnerabilities of the airports?

Mr. STEPHENS. They don't assess the cyber vulnerabilities of the airports. That is correct.

Mr. KATKO. What do you think about that?

Mr. STEPHENS. Well, you know, I think we can do a better job, as I said, across the sector. Right now, airports, airlines, and all other aviation sector components have a vested interest in doing it. We want to protect the traveling public. So we go above and beyond.

I would say that we are not the only ones across the industry. We do a good job. But if we are talking about partnering and making sure that there are clear command, controls, and communications between Government and the oversight agencies, as well as the airports in the sector, key components, then there needs to be a more urgent need to adopt some of those standards.

Mr. KATKO. Thank you, Mr. Stephens. Mr. Troy, Mr. Porter, you want to add anything to that?

Mr. TROY. I really—Mr. Stephens, I think I agree with his statements and he is well-positioned with his background, I think, to make those best observations.

Mr. KATKO. OK. Mr. Porter.

Mr. PORTER. Yes, I would agree and also—and deferring to Mr. Stephens. I think from other sectors, having those standards certainly does have an impact and raise its bar. It did in the finance sector. I think there is reason to think that it would in aviation, as well.

You know, for me, I want to make sure that any standards that are put in place not only focus on security, but resilience. Can the airport operate without internet access for a short period of time? Can people still, you know, do some basic level of operation? There will be some disruption no matter what, but I think that is an area that across all sectors, you know, we are falling beyond on as the opportunity to make sure that operations aren't totally disrupted when the internet or internet-connected device is brought down.

As long as we are held hostage by our technological and economic success, that is going to be a vulnerability, a strategic vulnerability for us as a Nation.

Mr. KATKO. OK. Mr. Chairman, just 1 quick second and a follow-up with Mr. Stephens. You are at Tampa Airport, correct? That is where you have your cyber systems that you oversee, correct?

Mr. STEPHENS. Yes, sir.

Mr. KATKO. All right. Why in God's name wouldn't the other airports be doing the same thing?

Mr. STEPHENS. Well, Chairman, I don't want to go as far as to say other airports aren't. I am sure that they are. But as I said in my written remarks, because of the governing structures in airports, so, for example, the largest airport, busiest airport in the world, Hartsfield-Jackson, that was referenced earlier, it is a subset of the city of Tampa, just like water and sewage—excuse me, of city of Atlanta, just like water and sewage.

Tampa International is an independent aviation authority, so we have more agility in implementing certain things. Another one, Chicago O'Hare, a subset of the city of Chicago. So when you look at it from that standpoint, airports are definitely doing things. I think they recognize the value for all the reasons that the other witnesses have mentioned. It is just that there is not necessarily a level of consistency.

As I pointed out, when that survey was conducted, only 34 percent had a baseline standard, and we have to do better as an industry.

Mr. KATKO. Thank you very much. Appreciate all your testimony.

Mr. RATCLIFFE. Thank the gentleman. The Chair now recognizes the gentlelady from Florida, Ms. Demings, for 5 minutes.

Ms. DEMINGS. Thank you so much, Mr. Chairman. Good morning to each of you. Thank you so much for being here with us today. Mr. Stephens, I welcome you from my home State of Florida.

As we all know, September 11 was one of the darkest days in American history. On that very dreadful day, I was assigned as a police commander to the Orlando International Airport. There is no doubt since that time we have really come a long way in terms of ensuring the safety of the traveling public.

But it does appear—and I am more convinced now than ever just listening to your testimony this morning—that the area of cybersecurity still appears to be or continues to be somewhat of a mystery. We still have much work to do.

I remember a long time ago as a law enforcement officer, we were told that you cannot fight today's battles with yesterday's weapons. As we have talked about, you know, some physical things that we have certainly kept up with to ensure the safety of our airports, cybersecurity just does not appear that we are quite there yet. But I am sure we will get there.

Mr. Troy, you were quoted recently in Bloomberg commenting on DHS and the FBI reports that Russian hackers attacked some aviation sector companies during assaults on U.S. critical infrastructure in 2017. In your view, have reports about State-sponsored attacks on aviation systems had a measurable impact on the way aviation sector executives view cybersecurity?

Mr. TROY. Yes, we have seen that the information that we have been able to share with the Government partners and amongst our member companies has absolutely driven them to up their game

with respect to their cybersecurity programs and in some instances actually reprioritize certain projects they were working on.

Ms. DEMINGS. I have also heard each of you talk about the importance of information sharing, and I know that there have been or continues to be some issues, especially between the public and private sector. You know, I have heard some say that the private sector is more willing to share information, but then the public sector are not so much.

So I would just like to hear from each of you—or perhaps Mr. Stephens or Mr. Troy—about what role do you think that DHS or the TSA can play in improving the information sharing or being more proactive in that area?

Mr. STEPHENS. So, Congresswoman Demings, I would start by saying that some of the information sharing that happens now, while it is good, sometimes it is not as fresh as we would like the information. Sometimes it is post facto. So I think they certainly can be more proactive.

There are certainly DHS resources that allow for information sharing—AIS, which is the automated indicator sharing system. But, again, those tools are out there, but how broadly disseminated they are to airports and to key aviation sector members is going to demonstrate the adoption of them and what their utility is going to be.

We actively look out there to see what tools are available. The resources that are out there from DHS we actively try to get everything that we can, where we can, but I think there has to be more proactive real-time sharing of information.

Finally, I would say one of the things that we are doing, for example, at Tampa International, in fact, today it is happening, our regional security director with TSA and our planning and development folks are meeting to look at how we can create our own threat fusion center where we have the airport operations center, CBP, TSA, other tenant agencies all collocated in one place.

In many airports, based on the structure, they are just simply not. Someone may be in discrete locations on the airport or maybe not even at the airport altogether. So I think more creative efforts to look at how we can break down those barriers to enhance information sharing is going to be critical to success.

Ms. DEMINGS. Mr. Troy, anything to add to that?

Mr. TROY. Yes, so as I mentioned earlier, I really like seeing DHS move into this risk management center. That really shows a strategic shift, which we think is critically important.

The sharing of information is only valuable when you are sharing information that is of value. That is one of the concerns that we have. We just don't want noise where the lots of indicators and the information moving across everybody and saying, wow, look, we are all sharing, this is great.

What we are looking for is kind-of a process that we use in the Aviation ISAC called risk registers, where we are actually looking to see what is really the biggest risks that you are worried about and where is there information that can help reduce those risks and close up those particular gaps.

So as Mr. Stephens mentioned, for example, there is many airports—and I agree with the statement, there are many airports

that really don't have a cybersecurity plan yet. It is difficult to understand how you can help someone who is not sure what their plan is.

So this process of helping people get their plans into place and then being able to use that information to develop the requirements for the types of information that can help them.

Ms. DEMINGS. Thank you. Mr. Porter, very quickly, anything to add?

Mr. PORTER. Sure. Nothing specifically on current information-sharing programs. I think it is just worth the subcommittee's considering and keeping in mind that the front line in the fight is going to be the private sector. I think if that were the guiding principle for, you know, Executive branch information sharing, it would be very different.

I think oftentimes it is viewed as an addendum to core responsibilities and not actually a core responsibility. But the fight is in overwhelmingly the private sector, private individuals, private companies, privately-owned infrastructure.

Ms. DEMINGS. Thank you so much. Mr. Chairman, I yield back.

Mr. RATCLIFFE. Thank the gentlelady. Chair recognizes gentleman from New York, Mr. Donovan, for 5 minutes.

Mr. DONOVAN. Thank you, Mr. Chairman. Being from New York, Mr. Stephens, I welcome you, too, because all my voters actually move down to you.

Mr. Porter, you made a great distinction between a tax that may inconvenience our travelers, whether it is the ticketing system going down, versus the things that might be dangerous or harmful to passengers. We had seen examples of someone with a laptop taking over one of these autonomous vehicles, driverless vehicles. Is that possible with an aircraft?

Mr. PORTER. That is not research that our company pursues independently. So I would have to defer to the aircraft manufacturers and the DHS report. I find the concern certainly credible enough that when our customers ask, we say that it is a credible threat, but we—you know, we generally refer that to specialists at the manufacturers or at DHS and others who have done the studies.

Mr. DONOVAN. I see. Mr. Troy, Mr. Stephens, do you have a comment on that?

Mr. TROY. So our members have not seen a credible report that has come in to them regarding the ability to hack a plane in a way that affects systems critical to flight. In my statement, I also said we don't know what we don't know. So the continuous monitoring, the continuous red-teaming, and the continuous process of safety integration of new systems constantly goes on in our industry to prevent that type of an attack from occurring.

Mr. STEPHENS. Congressman, I would agree with my fellow witnesses from an aircraft perspective, but what I would offer is the perspective—I used to be a former air traffic controller in the U.S. Air Force. What I would offer is the perspective of industrial controls for our NAVAIDs. I think that there are vulnerabilities potentially there, if you look at some of the studies, particularly as the FAA looks to moving toward next gen, right?

There is the ability potentially to spoof, you know, global positioning information systems. So there lies and exists a potential threat, whether we are talking about specifically on the aircraft, but certainly as the aircraft is approaching the surface where it needs to be able to land. We need to make sure that the same type of cybersecurity protections are in place for all of our NAVAIDs and all of our airport safety devices.

So that—from my perspective, that is why I think there is a particular more credible threat.

Mr. DONOVAN. Yes. You must be reading my notes. My next question was about the air traffic control system and someone compromising that while we have aircraft in the air, aircraft landing, aircraft trying to take off, and the dangers that would pose.

One issue if this happens when everything—every aircraft is on the ground, but I forget how many aircraft were in the air that fateful day that Ms. Demings spoke about that we had to put down on the ground, and if that system was compromised, how dangerous that would be.

This may piggyback on my first question and may be out of your realm, but in many of the things that we speak about on Homeland Security Committee, we talk about component parts. The compromising component parts is something that is put together elsewhere, whether our aircraft is built outside the United States or whether built here, but we have component parts coming in from outside, and if a compromised component part is built into the making of that aircraft, how dangerous that could be.

Are there measures in place to assure us that component parts would not jeopardize the aircraft after—while it is being made?

Mr. TROY. Yes, so our industry, again, is incredibly focused on safety. Even in the example of the information coming in through an air traffic control system, that is a single point of information coming in to the cockpit. The systems are not designed to rely on one piece of information or one source of information.

They are built in redundant ways in order to make sure that if a system did fail, there are ways to validate whether or not that system has failed and then other systems are in place to be able to leverage in those instances. That same process is also used with respect to the supply chain, so equipment is tested extensively, as it is put into each of the products.

You know, the products in the industry are much more than just the plane. I mean, there is many other products there. With the plane, again, the very high risk with anything that could impact critical flights, so there is going to be more of a—I would say more of a prioritization and more emphasis on those processes and that equipment.

Mr. DONOVAN. I thank you all. Mr. Chairman, I yield the remainder of my time back.

Mr. RATCLIFFE. Thank the gentleman. Chair now recognizes the gentleman from Rhode Island, Mr. Langevin, for 5 minutes.

Mr. LANGEVIN. Thank you, Mr. Chairman. I want to welcome our witnesses this morning. Thank you for your testimony. I think it is a very important hearing on an important topic.

So I was encouraged by the line of questioning and the answers on the—that Ms. Demings had raised about information sharing.

When we passed the CISA law in 2015, it was with the hope that we are going to bring down those legal barriers that existed, that were supposedly preventing robust threat indicator, sharing information from happening.

Unfortunately, now, 2 or 3 years later, we haven't—I think CISA has really yet lived up to what our hopes and expectations would be on info sharing. To date, there is only about 200 or so companies that are downloading information from DHS, that the Government is offering, and it is only about 6 or 7 companies that are actually sharing threat information back with the—to DHS.

So I find that troubling. Obviously, in an ideal world, we have robust information sharing of threat indicators, we had perfect situational awareness, we are going to go a long way toward better protecting our networks.

Mr. Troy, let me ask you. Again, I was encouraged by your testimony affirming the value of companies and Government agencies sharing information about cyber threats. So how active are the Aviation ISAC and your sector's members in DHS's automated indicator sharing program? Is the airline industry sharing cyber incident data with DHS?

Mr. TROY. So we have shared information with DHS numerous times over the past years that we are aware of that the Government actually turned it into an intelligence information report and the Government then shared that information amongst the Government. So we are proactively sharing with them, as I mentioned, information that we think is of value.

The Aviation ISAC itself is not involved in the automated indicator sharing program. However, we have some members who I believe are involved in that program with DHS. As, again, I mentioned, our focus is really trying to stay away from noise and be focused on key information that is critical.

Mr. LANGEVIN. Why do you think it is that more in the airline industry aren't more proactively engaged with DHS in the AIS system? What do you see as—I understand that, you know, you talked about not just sharing noise, but context. But what other things could we be doing to incentivize or ensure that more information sharing is actually going to happen from the airline industry?

Mr. TROY. Well, I think that the information that is of most value is getting shared. When information comes in, the way the Aviation ISAC works is that each member owns their data, so we ask them if they are willing to share this information beyond membership. We frequently get that thumbs-up from our members and are able to share that information with the Government.

The Aviation ISAC also has a person who reports daily to the NCICC and has access to our information, is able to have those conversations going on with respect to that information. So I think that, you know, the key pieces are in place there with respect to the sharing of information.

We are working with the DHS on what we think are some barriers to the sharing of information, and it has to do, really, with the classification of information by the Government. I, as was mentioned in my bio, I am former deputy assistant director of the cyber division of the FBI, so I am very familiar with the classifications

of information and the challenges of that, particularly in the cyber area.

I am constantly challenging the Government to take a look at information that it believes is—needs to be classified as cybersecurity information. A lot of the information that is obtained by the Government is in many, many places on the internet. Whether or not a source is at risk I think is a challenging question that we continue to push to see if more information could be shared.

Mr. LANGEVIN. Thank you. Mr. Stephens, let me talk to you about cyber incident reporting. You suggest in your testimony that the Government consider requiring disclosure of cyber incidents whether or not the incident resulted in a data breach or a system compromise. I couldn't agree more, actually.

So I discussed this issue more than once with respect to the transportation sector, and it is unfortunate to see the problem still remain. How would you hope that Tampa International Airport's ability to respond to cyber threats would improve if cyber reporting were mandatory across the sector?

You know, it is interesting how, you know, in perimeter security, if a gate were opened and a vehicle drives on to the tarmac, even if nothing happened and the vehicle turns around and mistakenly, you know, had gone onto the tarmac and turned around and left the perimeter, that incident would be reported. But if some—but if there were to be a cyber intrusion, even if the—in digital terms the perpetrator even made its way up to the plane or even put somebody on the plane, but nothing bad happened, I understand that that incident wouldn't have to technically be reported in terms of cyber terms.

Mr. STEPHENS. If it were a cyber incident, there is no mandate or requirement that I am aware of that that information would have to be reported. But what I would say, based on that comment that I made earlier about having a threshold, as the other witnesses have spoken, we don't want threat intelligence that just creates noise that is not actionable.

But say, for instance, something happens at Orlando International and there is a particular profile of a threat in the cyber space that happens there, there is a lot of utility for other airports within the State or within the region or the country to be able to have real-time access to that information. So sharing that information becomes extremely valuable from that perspective.

The other thing that I would say, again, with respect to no requirement on the Federal side that I am aware of, interestingly enough, most of the States have some data breach reporting requirement through their AG's office. In the State of Florida, there are certain triggers that require you to report data breach, for example.

So I think that there at least needs to be some strong consideration given to how do we do this in a way where airports and airlines and key stakeholders are more encouraged and more inclined to share that information in real time, or as close to real time as possible?

Mr. LANGEVIN. Thank you. My time has expired. I will yield back. Thank you, Mr. Chairman.

Mr. RATCLIFFE. Thank the gentleman. The Chair now recognizes the gentleman from Wisconsin, Mr. Gallagher, for 5 minutes.

Mr. GALLAGHER. Thank you, Mr. Chairman. Mr. Troy, you spoke briefly in response to a question about the challenges of sharing information between the Federal Government and a variety of entities. Then, Mr. Porter, in your written testimony, you mentioned that the best defense against cyber espionage is the rapid sharing of information to all concerned parties.

It seems that whenever we have hearings related to cyber, we all tend to land on or agree upon the idea that we need to do something to share information better, but because of the challenges you mentioned, we still haven't quite gotten there.

So beyond urging the Federal Government to be more discriminating with how it classifies information, and I share your sentiment. As a former human intelligence officer, I share the sentiments you express. Are there—for the whole panel, are there other steps you think we could take to enhance that sharing, which I think we all agree is critical?

Mr. TROY. Well, that is really what the Aviation ISAC has been set up for. We are very active out there in promoting our mission and trying to continue to develop increased membership. As I mentioned, we pass information out to the Government, and we also attend daily Government meetings, both through DHS and TSA, to share with them critical information when we have that.

I think the continued promotion of information sharing by the Government and the continued successes that we are seeing from the membership that we have at this point in time is driving more people to end up sharing more information and trying to get through, I think, some of the times that difficult decision of, do I want to let people know that I have been mugged in the park, so to speak?

There still is a hesitancy for people to share information about attacks. I personally believe that part of that is because of the potential for lawsuits that can come out of the sharing of information. That is an unfortunate consequence, because when you are trying to do the right thing, to share information with other people, to have a lawsuit follow on as to whether or not due diligence was in place in the protection of your system is a real challenge.

Mr. GALLAGHER. Thank you. Mr. Porter. No offense to your fellow panelists, but your tie is by far the best of the three.

Mr. PORTER. Oh, thanks, yes. So I guess when I think about information sharing, you are right. It is an easy plan to just say we should do more of it. But as some of the other panelists have noted, what the individual members of the aviation sector need is not more information. It is more relevant information.

The primary value that the Government is going to add is context. They don't—obviously, some of that may be very Classified and they can't share all of it. But much of the information is already going to be shared by private sector, cybersecurity companies like mine anyway.

What the Government can do is give you extra context, extra specificity, perhaps based on secret information. That is also what they are most reluctant to share, and rightly so. That information obviously could endanger sources if shared.

I guess my perspective is that that also describes counterterrorism reporting prior to 9/11. We don't want to wait until after a major incident to say that it is worth the risk. So we should be honest and say that it would be a risk to share that kind of context-heavy information. It would be a very real risk. But that it—at this point that it is worth it, because there is greater risk in not doing so.

I think as I mentioned earlier in my comments, the fact that the fight is primarily in the private sector, not in Government-owned networks, means that it is not going to ensure as a lasting solution for our country to focus all of our National defense resources just defending National defense networks. You are going to have push outward or it is not going to work. That will be a failure of then action that it will be difficult to assign blame, but there will still be victims for it.

So I think beforehand we should be proactive in saying we as a country understand the risk. It is a risk. We are going to do it anyway. So——

Mr. GALLAGHER. Mr. Stephens, do you have anything to add?

Mr. STEPHENS. Just simply this. I agree with Mr. Troy and Mr. Porter. I think the thing that the Government could do to facilitate that so there could be more real-time and ready accessibility to threat intelligence, actionable, relevant threat intelligence is perhaps creating a scheme where at certain critical infrastructure entities, such as airports, security clearances are granted to look at particular pieces of information.

Right now, there may be threat intelligence out there that may be very good for airports to know. But again, the classifications become a problem sometimes. Getting access in the real-time manner becomes the main obstruction.

Mr. GALLAGHER. It is very helpful. I am out of time, Mr. Chairman.

Mr. RATCLIFFE. Thank the gentleman. The Chair recognizes the gentlelady from Arizona, Ms. Lesko, for 5 minutes.

Ms. LESKO. Thank you, Mr. Chair, and thank you for all testifying today. I think, Mr. Troy, if I heard you correctly, you brought up that red teams are used. So, first, I want to confirm that my understanding of red teams are like the good guys that try to hack in to check for vulnerabilities. Is that accurate?

Mr. TROY. That is correct.

Ms. LESKO. OK. I guess I am trying to get an idea of what have you—your industry used red teams for? Have they tried to hack into the air traffic control system? Have they tried to hack into planes? How do you balance—I assume it is difficult to balance actually hacking in, because you might bring a whole system down. You probably don't want to do that. So how do you really test if something can be hacked into or not without bringing the system down?

Mr. TROY. So the FAA runs the air traffic control system, and we have not tried to hack it. Let me make sure about that. Our members use red teams on a regular basis. They give them full access. They allow them basically the ability to try and take down the systems, but not actual in-flight system. I mean, that obviously would be an issue.

Do they do tests in flight? Yes, they do tests in flight. Test flights, where they are doing work. But they conduct those systems—they use in-house employees, as well as they contract with specialists in the industry who hopefully come in with a different mindset, and used to the culture of the company that built it so that they can challenge their thinking and their systems, and they conduct those red team exercises.

But they are given full access to be able to actually find those vulnerabilities.

Ms. LESKO. Thank you. Mr. Chair and Mr. Stephens, you brought up an issue about the air traffic control system and possible vulnerabilities. It seems—can you expand a little bit more? Because we are modernizing the air traffic control systems, which right now, if—I think I went on a tour and they pass like tapes or something like that to each other, which, you know, isn't very modernized. But I assume that one of the risks of modernizing is that then it is more hackable. Am I correct?

Mr. STEPHENS. Yes, ma'am. That is the potentiality. Right now, as I referenced in my remarks, we are moving from a radar-based system, which is the current technology, even when I was a young air traffic controller, now to more a satellite-based technology with next gen. There are still system vulnerabilities with that.

In fact, the DOD has pointed out its concerns with next gen technology with respect to tracking military aircraft. So until we plug those vulnerabilities and fully understand, as the other panelists have said, we don't know what we don't know, there may be other things out there with the implementation of these systems that create problems for us.

I think from an industrial control system standpoint, things like NAVAIDs and airfield lighting and those types of things that are standard bread-and-butter operational types of structures, on every airfield, particularly at every commercial airport, those are the things that present some risk, whether it is broad-scale risk—as the witnesses have pointed out, there are redundant systems in place. But again, it only takes that one critical incident to really shock the psyche of the American traveling public. That is what we are trying to avoid.

Ms. LESKO. Thank you. Mr. Chair, I yield back my time.

Mr. RATCLIFFE. Thank the gentlelady. I want to thank all the witnesses for their testimony and thank all of the Members for their thoughtful questions today.

The Members of the subcommittees may have some additional questions for each of you. If so, we will ask you all to respond in writing. Pursuant to committee rule VII(D), the hearing record will be held open for a period of 10 days. Without objection, the subcommittees stand adjourned.

[Whereupon, at 11:32 a.m., the subcommittees were adjourned.]

APPENDIX

QUESTION FROM HONORABLE JAMES R. LANGEVIN FOR JEFFREY L. TROY

Question. What is it that motivates the Aviation ISAC's members to share threat and incident data, and how might more sharing be encouraged—even with the industry's regulators?

Answer. Great question! The answer is complicated and varies for each member.

The members are motivated to share because they recognize the cyber threat is universal and that the entire infrastructure is a target, not just one company. Our member companies take their security responsibilities very seriously and they view threat sharing as one of the ways in which they can work to better manage risk.

Trust is the most important element inducing members to share. We have a non-disclosure agreement (NDA) binding on all members. This agreement prohibits members from sharing information received from the A–ISAC or one of its members about cyber attacks on their networks or products.

However, an NDA is only a form. The real sharing only occurs when the members trust each other.

We have built trust through extensive leadership and community building. Our board member companies led the way in sharing without an expectation of return. They also took the risk of initiating the sharing early, when the trust was non-existent. They took the risk and led the way.

We built and maintain our trusted community by hosting in-person meetings. We do this at the executive and analyst levels. The CISOs have roundtable meetings in their regions. The analysts meet more frequently, 4 times per year, in person. We also facilitate daily exchange of information via our portal and slack channels. In addition, we have bi-weekly calls with the analysts. Frequent communication builds trust.

We are looking to increase sharing by creating more transparency in what is shared and how we develop that information. Celebrating the wins that come from sharing will drive more sharing.

This is not a perfect system. There is information that is not being shared. As I stated in the hearing, the threat of lawsuits inhibits sharing. A cyber attack can be equated to someone being mugged in the park. The victim is walking in what should be safe space. An attacker takes money and personal information by stealing the victim's wallet. The victim goes and tells the police, and now the police have the description of an attacker. The police may increase patrols in the park and warn others to be more aware. This may even lead reports from more victims.

Now take that scenario into the cyber world. A company network is attacked. Financial harm and proprietary information is stolen—but the attack is not always reported. Victim companies are concerned about being sued and the threat of more regulation which will bring cost, yet likely not increase the cybersecurity of the company. What would happen if victims in the park were worried they would be sued because they did not have strong personal security in place while walking in the park?

We must find a way to incentivize sharing by reducing the risk of lawsuits and over regulation. We need a way to harness market drivers that will enable affordable increases in security.

Nonetheless, the Department of Homeland Security, Federal Aviation Administration and the Transportation Security Administration are all working well with the A–ISAC. We have a person on the floor of the DHS NCCIC each day. This increases the sharing. Each successful share is driving more information sharing.

QUESTIONS FROM HONORABLE JAMES R. LANGEVIN FOR MICHAEL A. STEPHENS

Question 1a. You suggest that the Government consider requiring disclosure of cyber incidents "whether or not the incident resulted in a data breach or system

compromise." What definition of "incident" would you deem appropriate for operators?

Question 1b. How can we ensure that it is not over-inclusive in the way today's definition is vastly under-inclusive?

Answer. There are certain of cyber incidents that I believe rise to a level of criticality in airports that could impact one or multiple airports within the aviation system or that have an adverse impact on aviation security, aviation safety, life safety, or critical airport operations and airport performance. This category is potentially very broad and may include things such as disruptions to flight information display systems, baggage handling systems, as well as other systems that are essential to airport operations. These are the types of incidents that I believe should be disclosed with certain parameters that need to be developed, irrespective of whether the attempt resulted in a data breach or system compromise.

These types of incidents are to be distinguished from systems that while if disrupted through a cyber threat, the result may be passenger inconvenience or delay but operations, safety, or security would not be materially impacted.

The best way in my opinion to ensure that we are not over-inclusive is to allow airports in conjunction with, but not limited to, organizations such as the Airport Cooperative Research Program (ACRP) and Aviation–ISAC to propose or adopt general guidelines for reporting utilizing industry best practices.

Question 2a. Your testimony sheds light on how airports run on a variety of systems and networks—the airlines' ticketing and flight operations systems, the airport's ground support systems, the FAA's air traffic management systems, and dozens of vendor and support systems. How does this interconnectedness impact the cybersecurity risks of airports, and who is responsible for addressing the resulting overall risk posture or assigning priorities to those risks?

Question 2b. What might the TSA or FAA do differently to better oversee those cyber risks?

Answer. In my opinion, the interconnected nature as well as the prevalence of common-use technology amongst airport operators, tenants, vendors, and organizations such as TSA, FAA, and CBP, significantly impacts the overall cybersecurity risks of airports due to the sharing of information and the reliance of data from a multitude of interconnected systems.

Currently unless otherwise agreed upon, most of these stakeholders and entities are responsible for addressing their own overall cyber risks. However, virtually all airports play a significant role in mitigating risks presented by passengers, vendors, airline partners, and other key stakeholders through their own cybersecurity and threat prevention programs. The problem in my opinion is that some of these programs depending on the airport's resources are less robust and effective than others.

TSA and FAA can perhaps offer airports and aviation stakeholders with more proactive assistance in developing and implementing cybersecurity standards as well as proactively sharing key threat intelligence based recommendations that will allow airports to better mitigate risks from cyber threats.

Question 3. You suggest that the Government consider imposing minimum standards of security to the aviation sector. Is there an approach that TSA and the FAA might use to develop such standards that would encourage industry participation and buy-in?

Answer. It is my opinion that standards currently exist that can be easily adopted by airports and key aviation sector stakeholders to enhance their cybersecurity preparedness and resiliency. As discussed during the hearing, the NIST standard as well as the COBIT 5 standard offer excellent opportunities for airports to build robust threat mitigation and cybersecurity programs.

It is important to note that airports are very different with respect to their organization and operations and therefore a one-size-fits-all approach would be highly inadvisable and I believe ineffective. I believe that the TSA and the FAA can begin to more actively encourage airports to adopt and implement a standard of the airport or stakeholders' choice as a component of their System Security Plan. Airports stakeholders should be given the flexibility to adopt standards and mitigation measures that best fit their unique structures and risks.