FINAL REPORT OF THE AVIATION SECURITY ADVISORY COMMITTEE

IMPROVING CHECKPOINTS AT U.S. AIRPORTS

MAY 24, 2017

I.   FOREWORD

Aviation remains a high-profile target for terrorists seeking to do harm to the United States and the global economy. Passenger checkpoints at U.S. airports play a critical role in securing the traveling public from harm by screening passengers and their carry-on baggage to ensure that no prohibited items are allowed into the secure areas of airports or aircraft. Nevertheless, checkpoints can be source of frustration for travelers, who may have to endure long lines and intrusive searches, which can lead to anxiety and high stress. Crowded checkpoints can also serve as a vulnerable target.

The Aviation Security Advisory Committee (ASAC) is pleased to present industry and stakeholder recommendations to the Transportation Security Administration (TSA) outlining a vision of improved checkpoints at U.S. airports in the future. This report provides the key characteristics and components of an enhanced checkpoint, and specific recommendations for the Department of Homeland Security (DHS) and TSA on ways government can meet these goals.

II.   INTRODUCTION

This ASAC report on improving checkpoints at U.S. airports is the result of a provision in H.R. 636, the FAA Extension, Safety, and Security Act of 2016, which was signed into law on July 15, 2016. Section 3501 of that law directs the ASAC to "develop recommendations for a more efficient and effective passenger screening process." In developing the report, Congress calls on the ASAC to address the following considerations:

> A. The configuration of a checkpoint;
> B. Technology innovation;
> C. Ways to address any vulnerabilities identified in audits of checkpoint operations;
> D. Ways to prevent security breaches at airports at which Federal security screening is provided;
> E. Best practices in aviation security;
> F. Recommendations from airports and aircraft operators, and any relevant advisory committees; and
> G. "Curb to curb" processes and procedures.

This report also meets the provisions outlined Sec. 3304(a)(4) of the bill, which requests the ASAC to "provide recommendations on best practices for checkpoint security operations optimization."

A number of experts and organizations have already explored so-called "Checkpoint of the Future" (COF) concepts and initiatives. In developing this report, the ASAC endeavored to learn about key tenants of future checkpoint concepts; identify potential applications and opportunities for checkpoints in U.S. airports; and make recommendations to the TSA on how it can plan for and integrate improved applications and practices into U.S. checkpoints in the future.

The Security Technology Subcommittee of the ASAC took the lead in developing the report. The subcommittee held a series of meetings to understand previous work and concepts that have been developed regarding checkpoints of the future, and current initiatives underway within TSA, Customs and Border Protection (CBP), and the DHS to identify and implement improved capabilities at the nation's checkpoints. The Subcommittee then held a meeting with industry stakeholders and end users who provided perspectives on what they viewed as key drivers and capabilities needed at checkpoints.

After receiving government and industry input, the Subcommittee identified recommendations to the TSA Administrator specifying the key components of checkpoint enhancements in both the short and long term, along with recommendations on how the agency and DHS in general can meet these goals.

The ASAC would like to acknowledge and thank a number of contributors to the development of this report:

III.   EXECUTIVE SUMMARY

The Transportation Security Administration (TSA) has recently taken a number of substantive steps in a positive direction that should result in immediate and longer term improvements at checkpoints, presuming that the agency is appropriately resourced. However, aviation faces a persistent threat from terrorists that are constantly changing methods to circumvent security measures at checkpoints. In the future, checkpoints at U.S. airports must also be able meet the growing demand of air travelers and ensure that the highest screening capabilities and optimal operations are in place.

The TSA needs to stay ahead of its adversaries by constantly evolving screening checkpoints to account for known and anticipated threats, and it must be provided the financial resources to help meet its mission. The Aviation Security Advisory Committee (ASAC) believes that the TSA needs to redouble its efforts to drive innovation and improve checkpoints in a way that provides the highest level of security and convenience as possible, while at the same time respecting the privacy of travelers. In order to remain the world leader in aviation security, the TSA must set the vision for the future

checkpoint and create the roadmap to achieve this vision, and stay consistent in collaborating with government and industry to meet its mission.

To a large extent, checkpoints at U.S. airports remain very similar to the construct established in the mid-1970's. There are numerous opportunities to improve checkpoints to better detect current and future threats and improve the passenger experience. Key to improving the security and performance of checkpoints is knowing more about the passenger through Trusted Traveler programs and having the capacity to accurately verify their identity. Future checkpoints must have the capacity to dynamically screen travelers and their belongings according to their specific risk profile; feature robust automation and self-processing capabilities; and include enhanced technologies with improved threat detection and operational performance. Transportation Security Officers (TSOs) must be well trained and given the training and tools to help make their jobs easier and optimize the security and performance of checkpoints based on local situations.

The ASAC also recognizes that the privacy of the public must be protected in a transparent and understandable manner so that travelers do not lose faith in the security screening system.

The ASAC identified specific recommendations for TSA outlining how the agency can improve checkpoints at U.S. airports, including:

A. Increasing and stabilizing funding for TSA to improve checkpoints;
B. Maintaining consistent leadership within TSA;
C. Increasing the pool of trusted travelers;
D. Enhancing collaboration with other agencies within DHS;
E. Improving industry direction and engagement;
F. Improving the R&D and acquisitions process;
G. Networking the checkpoint;
H. Enabling TSOs to better perform their jobs; and
I. Enhancing international collaboration.

Section VIII of this report includes over 30 specific, detailed recommendations for TSA to consider.

Within this report, the ASAC focuses on key recommendations for TSA to achieve an enhanced checkpoint. However, Congress also plays a role in helping TSA succeed. In particular, *the ASAC recommends that Congress consistently fund the TSA at a level that will enable the agency to meet its mission and drive improvements at checkpoints in the future*.

One way to provide more resources to TSA is to cease the diversion of a portion of the 9/11 Passenger Security Fee paid by air passengers that is currently going into the general fund for deficit reduction, and dedicate this funding for aviation security activities. The ASAC believes that Congress should also provide direct funding to support TSA programs and initiatives to attract and enroll travelers in Trusted Traveler programs, and multi-year funding for checkpoint security projects, including the establishment of a capital fund for equipment similar to the one available for the Electronic Baggage Screening Program (EBSP). Finally, consistent and robust investment is needed in R&D, including giving consideration to establishing a consistent grant program for R&D activities to sustain vital research in future technologies with better capabilities.

IV.   **WHY DO WE NEED IMPROVED CHECKPOINTS?**

The U.S. has a vested interest in significantly improving checkpoints at airports. The U.S. currently serves as the world leader in aviation security, and checkpoints have been effective in preventing attacks on the aviation system. Nevertheless, the threat trajectory is evolving and airport security needs to stay ahead. Government investigations have outlined potential vulnerabilities at checkpoints and the potential vulnerability associated with large groups of passengers waiting at screening checkpoints are of concern. The ASAC identified the following reasons as to why checkpoints must be improved.

A. *Enhanced Security*
   The landscape of players and threats that seek to disrupt the U.S. and international aviation system are growing and ever evolving, as are the methods and materials available to carry out attacks, including internally-carried devices, novel new explosives, and repurposed everyday items such as laptops used as improvised explosives. Terror networks are on the rise and recruit through social media and other means. This makes the identification of threat actors critical, along with the validation of credentials used for travel. At the same time, home-grown, violent extremists who are self-radicalized and are independent of any directives from a central organization present an increasing threat. The growing sophistication of explosive materials and home-made explosives require higher capability screening equipment that can be updated quickly without long delays.

B. *Meet Future Travel Growth and Evolving Passenger Need*s
   Every day the TSA processes about 2 million passengers through checkpoints. The recent growth in the economy and relatively low oil prices have increased passenger traffic. ***However, TSA investment in staffing and technology have not kept pace with this growth***. In its most recent forecast, the Federal Aviation Administration projects that 1 billion passengers will fly in the U.S. by 2036. At the

same time, the demographics of travelers will dramatically shift in the future. Baby boomers will begin to retire and are expected to travel more, creating challenges relating to mobility within the checkpoints. Millennials on the other hand rely on technology and expect self-service in the travel experience. Many large hub international airports in the U.S. are currently close to or at capacity, are physically constrained, and unable to create new spaces or significantly enhance capacity.

C. *Wait Time Mitigation*
The growing delays at passenger checkpoints garnered much attention and press in the spring of 2016, prompting Congress to authorize TSA to reprogram funds to provide more Transportation Security Officers (TSOs) and overtime. Thousands of travelers missed their flights due to long queues and delays. Long lines and crowded checkpoints also create a higher stress environment for both passengers and security officers. At the same time, crowded checkpoints create a soft target for attacks that could occur on the non-secure areas of airports. More efficient checkpoints are needed to mitigate long lines and facilitate passenger throughput.

D. *Incorporate Better Screening Technology & Detection Capabilities*
Technology can play a vital role in meeting more advanced and ever changing threats, while also ensuring a pleasant and expeditious screening process. The TSA has been slow to test and deploy enhanced algorithms to improve the performance of existing equipment within checkpoints. At the same time, government and industry investment to develop the next generation technologies has lagged. Accelerated and advanced R&D and acquisitions are needed so that TSA has the most effective screening capabilities and airports can plan for the deployment of advanced technology in the future.

E. *Improved Operations/Utilization/Optimization*
Improvements should be identified to make checkpoints run more efficiently in the future. New terminal expansion projects should focus on flexibility of design to meet constantly evolving security screening procedures and new technologies. Checkpoints should also be modular to account for peak travel times of the day. The staffing of transportation security officers should be optimized through better allocations to meet peak demands. Federal Security Directors (FSDs), airlines and airports should be provided tools and options to make locally-based decisions to address busy travel times and seasons.

F. *Enhanced Work Force Environment and Engagement*
TSOs currently have one of the most difficult jobs available. Most work in a loud, stressful environment and face aggravated travelers. TSOs are required to do invasive pat downs to clear any alarms, and random pat downs of passengers have recently increased due to new threats. New technology capabilities and thorough

training will enhance the effectiveness of TSOs and create a more productive and secure checkpoint environment.

G. *Leverage the Opportunities Presented by Evolving Mobile Technology*
Basic screening methods and technology capabilities have not kept pace. In many respects, the checkpoint process is still based on the system set up in the mid-1970s. In particular, checkpoint security has fallen behind as it relates to taking advantage of the capabilities offered by mobile technologies. Smart phones are now almost universal and used by a growing number of travelers to reserve flights and to check in. There are opportunities to possibly use mobile devices to promote automation through security screening. For example, several states currently have pilots in place that are exploring the feasibility of allowing residents to carry their driver's license in a smart phone. The American Association of Motor Vehicle Administrators is currently developing a standard that includes biometrics and the ability to communicate electronically with trusted entities to confirm identity. Such technological improvements could not only be leveraged to confirm identity at the checkpoint (thereby increasing security), but also remove the need for a Travel Document Checker, saving TSA money and provide for faster screening. However, standards for enrollment vary between the states and TSA should review how a state issues a driver's license, and whether that process is secure.

V.   STATE OF PLAY: INITIATIVES UNDERWAY AT DHS/TSA

In preparing the report, the ASAC Security Technology Subcommittee requested briefings on current and planned initiatives underway at DHS and TSA. The Subcommittee heard about a number of activities to address short- and long-term improvements at U.S. airport checkpoints.

Key initiatives underway at the TSA include the following:

A. *Risk Based Security*
TSA's Risk-Based Security (RBS) began in 2011, and was an underlying principle to transition the agency away from a one-size-fits all screening regime to one that focuses on higher-risk passengers. This has been a key driver in incorporating improvements into checkpoints by enhancing the pre-screening of travelers and creating a significant pool of known, vetted travelers. RBS principles must continue to drive all TSA decisions, as noted in its 2015 *Strategic Five-Year Aviation Technology Investment Plan,* where TSA envisions "a future defined by intelligence-driven, risk-based screening procedures and enhanced technology

that will enable TSA to employ a flexible, adaptable, and robust multi-layered approach to detecting an evolving range of threats."

B. *TSA Pre✓® Program / Trusted Traveler Programs*
TSA's Pre✓® Program is the most visible RBS program offered by the agency. Under the TSA Pre✓® Program, travelers are vetted and have access to separate lanes for expedited screening. TSA Pre✓® Program travelers do not have to take off shoes and are able to keep laptops in their cabin bags. Other Trusted Traveler programs are available including Global Entry. These programs are a key driver to help differentiate travelers and their screening requirements based on their risk profile. Efforts must continue to enroll as many travelers as possible in these programs.

C. *Operational Baseline Assessment*
TSA has undertaken a comprehensive review of its operations at checkpoints. Through this initiative, the TSA found opportunities to enhance tools available to local field management to optimize staffing, improve credentialing and biometric capabilities, and increase technology capabilities, both in the short- and long-term.

D. *Innovation Task Force & Partnerships*
In 2016, TSA unveiled the Innovation Task Force (ITF) to help mitigate growing delays at security lines across the country. The ITF's mission is to "foster innovation by integrating key stakeholders to identify and demonstrate emerging solutions that increase security effectiveness and efficiency, improve passenger experience, and deliver the next-generation of curb-to-gate passenger experience." To date it has focused primarily on the deployment of automated screening lanes, which have enhanced security while increasing passenger throughput by 20-30 percent. Under the program new, more capable technologies will be placed at airports across the country to assess and ascertain the effectiveness of the equipment in an operational environment. It is encouraging industry and government to work together to develop integrated solutions that will enhance the passenger journey. With appropriate funding, the ITF should help to provide TSA and industry an opportunity to examine new generations of screening equipment, new processes and checkpoint configurations, and will help formulate the requirements for a potential acquisition process. The ASAC strongly supports programs like this that will help to drive innovation at checkpoints.

E. *APEX Screening at Speed Program*
The DHS Science & Technology Directorate (S&T) launched its APEX Screening at Speed program, in collaboration with TSA. The program has helped to identify TSA's capability gaps and technology needs in the longer-run. In accordance with

RBS principles, the vision is to develop deployable aviation security checkpoint technology that screens 300 passengers and their carry-on belongings per lane, per hour at a high detection level with dynamic adaptation and no divestiture of liquids or electronics.

F. *Engagement with Customs & Border Protection*

The ASAC welcomes recent efforts by the TSA and Customs and Border Protection (CBP) to explore opportunities by working together to enhance the entire passenger journey. CBP has made notable strides in automating customs processing for international travelers that significantly enhance self-service. CBP has advanced passenger manifest information and is exploring ways to use biometrics to verify identity and get away from using documents altogether, allowing travelers to self-process through kiosks. TSA and CBP should endeavor to identify and utilize similar biometric and authentication capabilities and share passenger data to enhance processing during all facets of the traveler journey, while recognizing the privacy and civil liberties implications associated with biometric collection and use. CBP is currently working to develop the Biometric Verification Service (BVS) which, at a minimum, would allow trusted partners such as TSA to biometrically confirm the identity of foreign visitors, thereby removing the need for the travel document checker. Taken a step further, BVS has the potential to leverage the vetting completed by the State Department and CBP to segregate those travelers into a known traveler lane such as the TSA Pre✓® Program.

G. *International Collaboration*

TSA has undertaken efforts to better coordinate and share information with international agencies. Specifically, TSA has discussed threats and opportunities to jointly define security equipment capabilities. With the passage of U.N. Security Resolution 2309, member states are called upon to strengthen security screening procedures and maximize the use and sharing of new technologies and innovative techniques that maximize the capability to detect explosives and other threats, as well as to strengthen cooperation, collaboration, and share experience in regards to developing security checkpoint technologies. In addition, the resolution recognizes the requirement for airlines to provide advance passenger information to national authorities.

TSA has also visited international airports across the world to examine unique checkpoint configurations and new technologies. These visits have resulted in new technologies being fielded here in the U.S. under the TSA's Innovation Task Force. The International Air Transport Association (IATA) and Airports Council International (ACI) have jointly implemented a program for airports to identify and test checkpoint innovations under their Smart Security program. TSA also

continues to coordinate with the Canadian Air Transport Security Authority (CATSA), which is implementing checkpoint of the future concepts at its airports.

VI.   CHECKPOINT OF THE FUTURE: WHAT IS IT?

Over the years there has been much focus on ways to enhance passenger security checkpoints at airports. One of the earliest concepts was the "Checkpoint of the Future" program developed by IATA in 2010. This program has evolved over time and currently falls under the "Smart Security" Program administered by IATA and ACI.

The Smart Security program "envisions a future where passengers proceed through security checkpoints with minimal inconvenience, where security resources are allocated based on risk, and where airport facilities are optimized, thus contributing to an improved journey from curb to airside." Key drivers of the Smart Security program include risk-based security concepts, advanced screening technologies and process innovations. Hartsfield Jackson Atlanta International Airport is the first U.S. airport to participate in this program.

The ASAC researched these programs and received briefings on a number of initiatives underway at TSA. The ASAC also invited a number of U.S. aviation stakeholders to provide recommendations on what they believed were key improvements that needed to be made at U.S. checkpoints. Based on these inputs from diverse stakeholders, the ASAC identified central drivers of improved checkpoints at U.S. airports that will increase security and the facilitation of passengers.

Key Drivers of Improved Checkpoints:

A. *Passenger Biographic and Biometric Data*
    Risk Based Security must continue to be a central driver to improve security at airports. While the focus of the ASAC report and recommendations is on passenger security checkpoint at airports, much of the opportunity to enhance performance and improve the passenger experience will rely on the information and data voluntarily gathered about the passenger well before they arrive at the checkpoint. ***A key enabler to improving checkpoints lies in knowing more about the passenger, verifying that they are who they say they are, and subsequently having the capability to screen the passenger and their belongings based on their specific risk profile.*** Indeed, this driver to improve checkpoints at U.S. airports will facilitate the entire passenger travel experience. The pool of air travelers that are participating in known-traveler programs must be expanded to help get more passengers into expedited screening lanes.

B. *Reservation to Destination Security*
There is an inherent risk in having a single point of failure by relying on the checkpoint to identify and remove threats. Security should begin at the point the reservation is made, to arrival and check-in at the airport. Opportunities should be identified to diffuse security out from the checkpoint into the entire airport terminal.   Technology must work in conjunction with terminal design and operational strategies to start the checkpoint security screening process right when the passenger arrives.

C. *Dynamic Screening*
Checkpoints need to be adaptable to account for passengers of different risk levels that need to be screened. Screening equipment should be capable of adjusting detection algorithms on the fly, depending on the individual risk profile of passengers and the flights they are taking.

D. *Automation*
Providing the passenger with the capability to manage and control as much of their journey through the airport terminal and checkpoints as possible will reap benefits in enhancing checkpoints at U.S. airports. Automating the passenger check in and screening process will optimize the utilization and effectiveness of the screening staff to accomplish their core functions and help to control costs.

E. *Enhanced Capabilities*
Improved technology must be developed and fielded to provide better detection and operational capabilities at checkpoints. Such technology must be able to authenticate and screen passengers and their cabin baggage with little to no divestiture, with low false alarm rates, and improved user functionality and interface. TSOs must also be able to better understand and have the capacity to use the equipment as well. Future technologies should be networked to screen passengers and their belongings based on their specific threat profile, and to be upgraded with the latest detection algorithms.   The networked checkpoint systems must be hardened against cyber-attacks and vulnerabilities.

F. *Consistent vs. Random Security*
There is an inherent tension between providing passengers a consistent security screening process, yet not having a static checkpoint system which can be studied for vulnerabilities and potentially compromised. Passengers have expressed frustration with screening procedures that can vary from airport to airport. Passengers need to expect and understand the security procedures that will take place at the checkpoint, and the fact that they may be applied in different ways and at different times from airport to airport.   Random use of passenger engagement and handheld trace detection systems, fluctuating detection

algorithms, and other tactics and technology can prevent actors from learning how to compromise checkpoint systems. Screening by canines should be increased to supplement checkpoint security. Random patrols of law enforcement officers can also serve as a deterrent.

G. *Well-Trained, Customer-Oriented Security Officers*
The key mission of TSOs is to secure the traveling public from threats, and they are asked to accomplish this in a stressful environment filled with anxious passengers. However, the key objective of meeting security requirements does not necessarily have to conflict with fostering improved interactions with passengers. This will help create a more productive and calming screening experience for both officers and passengers. TSOs should be provided enhanced training to gain a full understanding of the checkpoint screening technology in addition to customer service-oriented training.

H. *Privacy Protective Approach*
Corresponding with a need to improve and enhance the security of the screening process, the government has an obligation to stakeholders to ensure that the collection, use, and disclosure of personal information is done in a manner consistent with the needs for security. Government must communicate with stakeholders in a transparent and understandable fashion, and address options for travelers to provide choices. At the same time, government needs to maintain personal information in a manner that is surrounded by appropriate controls to prevent unauthorized or improper access. Finally, government must minimize the information necessary for ensuring the mitigation of relevant risks.

Privacy is a specific obligation of TSA through the need to perform a Privacy Impact Assessment of any new or enhanced processes under the requirements of the DHS Privacy Office and existing legislation. Notably, processes and initiatives that are seen as privacy protective will encourage participation by the traveling public and help ensure both the sustainability and the effectiveness of that process in the long run.

These drivers provide the underpinnings of a vastly improved checkpoint at U.S. airports and help to enable numerous opportunities to enhance security and passenger facilitation. With these serving as the backbone of an effective checkpoint, there are certain components that help create an efficient checkpoint process. The ASAC asked stakeholders to provide recommendations on what U.S. checkpoints in the future should look like, in terms of design and equipment used in the space. Based on inputs from these stakeholders, the ASAC identified the following components.

Key Components of Improved Checkpoints:

A. *Checkpoint Layout*
Terminals should have good wayfinding and signage so passengers can easily find the checkpoint as they walk into the terminal. Terminal plans and designs should offer the greatest flexibility possible for evolving checkpoint configurations and technologies. Designs, materials and environmental strategies can be used to create a calm checkpoint. Soft colors and lighting, living plants, and acoustic enhancements can reduce the industrial noise that normally accompanies checkpoints. The checkpoint space should be modular and easily shift to accommodate peak rush-hour traffic or slower times of travel.

B. *Wait time information*
Clear and accurate information regarding wait times at checkpoints is an important tool to relieve traveler stress. This information should be available prior to the arriving at the terminal, and be easily accessible at the terminal itself. Information should convey checkpoint wait times and directions to other, less congested lanes or checkpoints when possible. Along with wait times, communication within the checkpoint should be dynamic and clearly available on why screening is important and instructions for passengers to make the process better.

C. *Passenger Self-Processing*
Remote check-in, remote bag check-in, self-bag tagging, and other automation mechanisms will relieve crowds before checkpoints. When gaining access to checkpoints, to the extent possible, the process should move away from presenting documents to deploying technology that will accept biometric data to authenticate travel information and the identity of passengers entering security checkpoints. A majority of passengers should be able to transit through the checkpoint without the need for verbal instructions by or direct interface with TSOs.

D. *Traveler verification*
Travelers should be able to use kiosks to self-verify their identification using a biometric reader. Biometric technology error rates must be reduced to an acceptable level. This can eventually trigger the dynamic protocols and the risk-level at which each passenger will be screened as they proceed through the entire checkpoint.

E. *Entering/Exiting Screening*
Separate parallel stations will allow passengers to simultaneously divest and prepare for screening at their own pace. Bins for carry-on baggage should contain

an RFID chip to track cabin baggage as travelers progress through screening. If any bag should cause an alarm, the bin is removed from the line for more thorough review and does not delay the screening of subsequent items. Bins are automatically returned to the front of the line. Space is available away from the checkpoint for private secondary screening and false alarm resolution, and to allow for self-paced and convenient re-composure at the end of the screening line.

F. *Screening Technology*

In a truly dynamic checkpoint, the screening equipment has the capacity to change to a lower detection threshold if the passenger is a known and vetted traveler, while a non-vetted or high-risk passenger would experience higher detection calibrations as they are processed through checkpoints. This could occur within the same screening lane. Technology should be implemented to track and match the passenger to their belongings through the entire checkpoint process. Next-generation equipment should enable less divestiture by passengers while reducing false alarms, allowing for less secondary screening and intrusive pat-down searches. Walk-through passenger screening equipment will alleviate the need to pause for screening. Carry-on bags should be screened with the latest technologies that allow passengers to keep their laptops, liquids and gels in their bag. Both passenger and cabin baggage screening equipment should increase automation to the maximum extent possible. Examples are expanding the use of Automated Threat Recognition algorithms to potentially include weapons and prohibited items, and exploring the use of non-contact trace detection for both primary and resolution screening to minimize hands-on contact. Detection algorithms should automatically be set for the screening equipment at a level commensurate with a passenger's risk profile. The equipment must be easier for TSOs to use. At some airports, centralized processing rooms can allow security screeners to examine images from bags in a remote facility away from the checkpoint, separating them from the din and bustle of the checkpoint and allowing better concentration on finding unauthorized items.

VII. THE ROLE OF PRIVACY

Much of the public discussion around enhancing U.S. checkpoints focuses on the issue of privacy and, more specifically, issues related to the collection, use, and disclosure of passenger data. While the availability of passenger data is an enabler to improve checkpoint security and performance, without ensuring protections for privacy, individuals may not decide to share personal data to receive expedited screening, and growing the pool of vetted travelers will continue to prove challenging.

The ASAC recognizes that the privacy of the public must be protected in a transparent and understandable manner so that travelers do not lose faith in the security screening system. Put another way, protecting privacy and civil rights does not necessarily conflict with enhancing security and, by gaining the trust of the public, may improve the effectiveness through greater participation and permissible coordination. Privacy includes strictly limiting the use of passenger information to aviation security purposes.

Passenger data containing personal information is collected, used, and disclosed across the entire spectrum related to air travel. Currently, TSA, CBP and other U.S. government agencies all access different types of passenger data. Additionally, airlines also collect and access a tremendous amount of personal information from their customers. Travel agents, retailers, facilities as well as international agencies and businesses collect and interact with passenger data as part of the travel environment. At this time, there is a lack of coordination and limited opportunity to share data to enable true risk-based security, and make sure that the right people receive the right data, at the right time. To have this become a reality, privacy protections must be embedded to provide confidence, both to travelers and the participating parties, that this is done in the "right way."

Although it has been argued that privacy concerns have limited opportunities to improve security, such as screening equipment with the capacity for much more realistic imaging resolution that has been scaled back due to privacy concerns, privacy and security are not a zero-sum situation. Travelers are rightly concerned about access to their personal information – when it's accessed, used, stored, and shared. Also, they worry about data breaches and most trust the private sector more than government in securing and maintaining the confidentiality of personal information.

The government must play a leading role in establishing the proper framework for the security environment addressing the collection, use, and disclosure of passenger data in a way that is sensitive to privacy concerns.

VIII. HOW TO GET THERE: ASAC RECOMMENDATIONS

The ASAC has identified the following key recommendations on how the TSA can position itself to develop and deploy a more efficient and effective passenger and baggage screening process. TSA should identify which recommendations would require Congressional action or could be done through executive action.

A. *Increased, Stable and Dedicated Funding for TSA*

The U.S. is challenged by the lack of funding available to improve checkpoints. In the interest of national security, the U.S. Government plays a critical role in

funding checkpoint screening technology and staffing. However, annual budgets and appropriations for the TSA, similar to other federal agencies, have been inconsistent as it relates to funding levels and timing.

Through the Aviation and Transportation Security Act (ATSA), the legislation that created TSA, Congress directed the agency to impose a "fee" (9/11 Passenger Security Fee) on passengers "to pay for the following costs of providing civil aviation security services." In addition to being used for to help offset the costs of the salary, benefits and overtime for TSOs, their supervisors, managers, etc., the fee is supposed to be used for "the acquisition, operation, and maintenance of equipment used by such personnel."

However, Congress, through the Bipartisan Budget Act of 2013, directed the diversion of an increasing amount of the 9/11 Passenger Security Fee each fiscal year through 2023. In the current fiscal year, $1.28 billion of the fee will be diverted to non-aviation security functions such as debt reduction.

According to TSA, $3.69 billion was collected in FY 2016. However, roughly more than a third ($1.25 billion) was diverted to reduce the national debt. This constrains the TSA's ability to full fund security activities at airports both now and in the future, and the ASAC strongly recommends that revenues derived from the fee should be used for its intended purpose.

At the same time, TSA has yet to provide Congress or industry a clear number that outlines the necessary funding and resources the agency needs to meet its mission and substantially improve airport screening, and to keep pace with the growth in passenger traffic. TSA will also need to ensure that the currently deployed equipment, which is getting older and becoming obsolete, will be recapitalized in the future. Recapitalization plans for existing equipment at checkpoints are constantly shifting and changing, and there is no clarity on how TSA will transition to the next-generation of screening equipment.

Recently, airports and airlines have provided substantial resources to integrate new technologies into checkpoints under the Innovation Task Force. However, industry simply cannot sustain the investment in screening technology that should be procured and deployed by the Federal Government.

> **Recommendations:**
>
> A.1   Notwithstanding current or anticipated future budgets and spending levels, identify the full funding requirements needed to transition to a checkpoint of the future.
>
> A.2   Formalize and determine the future of the Innovation Task Force. Detail a plan to fully resource the initiative and the rules of engagement for industry to participate.

B. *Consistent Leadership within TSA*

The frequent changes in TSA leadership and staff turnover have substantially challenged the agency's ability to identify and implement needed reforms. The changes in leadership have resulted in shifting focus areas, and initiatives and programs that have been introduced and subsequently languished. Attempts at process reforms have led to frequent reorganizations and overall institutional instability.

> **Recommendations:**
>
> B.1   Enable and identify individuals/positions within the TSA that will have ownership and decision-making authority over aviation security effectiveness, including the technology development, acquisitions process ownership, cybersecurity implementation and operations, and privacy expertise.
>
> B.2   Detail how the recent reorganization of the TSA will help meet the objectives outlined in this report, and how it will facilitate improvements to the transportation security equipment development and acquisitions process.

C. *Increased Pool of Trusted Travelers*

While there has been progress in growing the pool of TSA Pre✓® Program and other known traveler programs, target goals have fallen well short of reality. Increasing the pool of vetted travelers can substantially enhance opportunities to increase security and passenger facilitation at checkpoints.

> **Recommendations:**
>
> C.1   Grow the TSA Pre✓® Program to capture over 30 percent of air travelers by 2020.

> a. Identify the resource requirements, staffing, and budget required to substantially increase marketing activities to encourage more travelers to sign up, focusing on educating the public on the benefits of enrolling.
> b. Expand the use of public/private partnerships (P3) to market the program.
> c. Accelerate participation by leveraging and marketing the availability of existing enrolment platforms, and launching a program to use the application capabilities of P3s to expand enrollment opportunities for travelers.
> d. Focus efforts on signing up occasional travelers and Millennials.
> e. Explore options such as providing group or bulk discounts, corporate incentives, etc.
> f. Consolidate Trusted Traveler programs available within DHS.
> g. Develop a universal enrollment website that is more user friendly and directs travelers to the appropriate trusted traveler program.
> h. Offer passengers the opportunity to sign up for the TSA Pre✓® Program for a single trip.
> i. Consider allowing international travelers that have been vetted by CBP and have used Automated Passport Control (APC) kiosks to use the TSA Pre✓® Program.
>
> C.2 Engage the TSA and DHS Privacy Offices in providing input regarding privacy protections to increase public trust in program operation.
>
> C.3 Develop a plan to ensure TSA, airports and airlines are prepared to handle increased participation in the TSA Pre✓® Program and more passengers using the TSA Pre✓® Program lanes to prevent frustration with increased wait times in these lanes, which could potentially compromise long-term, sustained growth in the program.

D. Enhanced Collaboration Within DHS

Internal to DHS, there have been institutional silos that have impeded opportunities to address security capability gaps and identify technologies and processes that would enhance the entire passenger experience at airports.

Government should identify the key performance metrics of checkpoint performance and technology, along with necessary resources to ensure that programs and initiatives are fully funded and staffed. Better intergovernmental coordination should be fostered to identify standards and reduce the duplication or divergence of technologies and practices related to the processing of passengers at airports.

> **Recommendations:**
>
> D.1   Identify and document the statutory and regulatory policies in place that potentially inhibit opportunities for collaboration and alignment within DHS agencies, including TSA and CBP, to improve checkpoints.
>
> D.2   Coordinate with other DHS agencies, such as CBP, to help improve the facilitation of passengers throughout the entire journey.
>
> D.3   Establish a standard for sharing and using passenger data among airlines and agencies that operate in airports.
>
> D.4   Establish a unified roadmap between TSA, CBP and S&T regarding the use of biometrics and technologies to enable biometrics at checkpoints and airports in general.

E. *Industry Direction and Engagement*

TSA needs to take a leadership role – in coordination with international partners - to define the specific detection and performance requirements and standards to improve checkpoints. TSA should also be more transparent and engage with industry by fostering opportunities for collaboration to identify and implement improvements at the checkpoint. Innovative solutions and funding mechanisms should be identified to test and sustain checkpoint improvements.

> **Recommendations:**
>
> E.1   Establish service quality standards and metrics to identify the level of performance that passengers, airports and airlines could expect and are receiving from the next generation checkpoint. The following aspects of performance within the next 10 years should be included:
>
>   a. Passenger satisfaction with the overall security screening experience;
>
>   b. Wait time performance with the expectation that 95 percent of all passengers will be screened within 5 minutes of arrival at checkpoint;
>
>   c. Wait time performance with the expectation that 99 percent of all passengers will be screened within 10 minutes of arrival at checkpoint;
>
>   d. Electronic data exchange response standard for queries of airline passenger data systems.

E.2　Foster collaboration among industry and incentivize competition, including promoting integrated solutions to improve the overall performance of checkpoints.

E.3　Identify specific steps to increase transparency and collaboration between government and industry on threats, capability gaps, and government needs, including further development of the Transportation Security Capability Analysis Process (TSCAP) and engagement with industry.

E.4　Regularly update industry on key performance requirements including detection standards. Updates to industry should include timelines for planned implementation/enforcement of requirements.

E.5　Divest more decision-making authority to local FSDs, airlines and airports to make informed decisions that will improve checkpoint performance and increase the security of the traveling public.

E.6　Identify technology and techniques that provide FSDs, airports and airlines the ability to make local decisions to improve checkpoint performance.

E.7　Engage with privacy and information security professionals to give insight into best practices to safeguard personal information and address protections for collection, use, and disclosure of information.

F. Improved R&D and Acquisitions Process

It currently takes far too long for new technology capabilities to be developed and deployed at airports. The testing, evaluation and acquisitions processes are time consuming and expensive for both government and industry. TSA has been reactive to threats and has not communicated effectively to industry the specific performance capabilities and gaps it seeks to improve, and set standards for industry to meet.

TSA has been challenged by inconsistent funding appropriated for checkpoint improvements on a year-to-year basis, along with having to respond to shifting threats and changing priority areas. Industry dynamics have also prevented opportunities to improve the performance of checkpoints across the country. The industry has recently experienced a spate of mergers and consolidations, as the domestic security market has been challenged by uneven funding and procurement plans. The lengthy and expensive process of getting equipment certified and qualified by TSA inhibits new companies from entering the market. It can take 5-10 years to navigate a new piece of equipment from development to deployment, and can cost tens of millions of dollars.   As a result of these circumstances, more companies are chasing opportunities abroad.

Industry needs more information and direction from TSA to ensure future investment, manufacturing and R&D plans are aligned with government needs.

Recommendations:

F.1 Develop and share with industry detailed and reliable spend plans for equipment recapitalization and new technology acquisitions.

F.2 Collaborate with S&T on identifying capability gaps and work in alignment to define and develop new capabilities.

F.3 Strengthen the development of key detection and operational requirements for equipment.

F.4 Improve the test and evaluation process to make the process more efficient and less expensive.

F.5 Provide industry the status of cybersecurity, Open Architecture, and other programs, specifically the timeframes and plans for future implementation.

F.6 Engage the TSA and DHS Privacy Offices in the development of plans to incorporate privacy protection into design and development as well as deployment.

F.7 Modify the Innovation Task Force mandate to conduct quarterly collaboration meetings with industry, building on the model from the Security Equipment Integrated Product Team (SEIPT), a government/industry partnership that was formed to collaborate on innovative security technology evaluation and deployment.

F.8 Accelerate the certification and deployment of canines at checkpoints.

   a. Add capacity to TSA's canine training facility.
   b. Develop a third-party canine certification program.
   c. Update and share with industry checkpoint design standards that account for the increased use of canines.

F.9 Enhance TSA's ability to invest in research and development to mature low technology-readiness-level (TRL) capabilities that will support acquisition and deployment across the transportation security enterprise

F.10 Implement a faster development cycle:

    a. Detail how the ITF is informing and will improve the acquisitions process.

    b. Expand the ITF and broaden opportunities for airports to test new equipment for those not participating in ITF programs.

    c. Share key performance data from ITF-sponsored projects and checkpoint enhancements with industry stakeholders.

    d. Provide industry early access to real world environments to understand and refine technical operations and human factor issues

G. Network the Checkpoint

A key enabler for an efficient checkpoint is having the capacity to dynamically change the detection algorithms of equipment based on an individual's or flight's risk profile. Networking the checkpoint can help make this happen. It will also keep screening equipment updated to meet evolving threats through an open architecture system that would facilitate automatic updates to equipment. TSA must protect this system of systems from cyber-attack vulnerabilities by establishing standards and sharing them with industry.

Recommendations:

G.1 Develop requirements and implement the Security Technology Integrated Program (STIP) program to network equipment, and an open architecture system to allow for dynamic screening and automated algorithm updates. These standards need to be incorporated into future contracting vehicles.

G.2 Identify, establish and share with industry cybersecurity requirements as soon as possible to enable a networked checkpoint.

H. Workforce Considerations

The TSA must enable transportation security officers to better perform their jobs and develop a checkpoint environment and culture that will enhance the utilization and capabilities of staff to be as effective as possible in detecting threats. To the extent possible, TSOs should treat passengers as customers and provide friendly service to help alleviate stress and to create a more effective checkpoint environment.

Disruptive technological tools should be developed that support the TSA workforce in carrying out the vitally important task of physical screening. The screening procedures and equipment should be easier to understand, learn, and implement. User interfaces need to decrease workload and utilize common, simple to understand interfaces. Such

focus will result in technology that supports continuous improvement in the workforce and help understand the performance of screening equipment.

Recommendations:

H.1   Ensure TSOs are well trained on checkpoint procedures, technology capabilities, alarm resolution, and ConOps.

H.2   Provide training in customer service techniques and passenger interface strategies that also incorporates privacy, disabilities and multicultural awareness.

I. Enhanced International Collaboration

The ASAC believes that the TSA can achieve tremendous opportunities in increasing security for aviation and airports in general by fostering international collaboration and information sharing. Efficiencies can be gained by working to identify and share information about threats, collectively determining equipment detection and operational capabilities, and data sharing. The TSA must continue its leadership role in setting the standard for security, but also leverage practices and technologies that are currently being implemented at international checkpoints.

Recommendations:

I.1   Conduct meetings with EU and other countries with the objective of reaching alignment on the sharing of information regarding threats and countermeasures.

I.2   Conduct meetings with the EU and other countries with the objective of aligning screening procedures, equipment detection and operational standards, and equipment testing and certification.

I.3   Specify how TSA will meet the information sharing directive outlined in UN Resolution 2309.

IX. Closing

TSA's core mission is to "Protect the nation's transportation systems to ensure freedom of movement for people and commerce." The aviation system remains the highest profile target for attacks, and in many respects the checkpoints at U.S. airports are the last step in detecting and deterring terrorists from entering the system. While checkpoints have been effective in preventing attacks on the aviation system, the TSA must take steps to improve and enhance checkpoints to meet evolving threats and the anticipated growth in air travel.

In developing this report, the ASAC examined current and future initiatives underway at TSA and DHS, and collected information and recommendations from a diverse set of aviation stakeholders and end-users on checkpoint performance and opportunities for improvement. Industry provided a vision of future checkpoints with increased capabilities and improved passenger facilitation, and offered specific recommendations on how TSA can achieve this vision.

The ASAC stands ready to work with TSA on meeting the vision and recommendations outlined in this report, and looks forward to identifying next steps and a path forward to meet this vision.

Appendix

Report Development and Contributors
The ASAC would like to acknowledge and thank the numerous individuals that contributed to the development of this report, including:

Report Co-Leads:
- T.J. Schulz, Airport Consultants Council; Co-Chair, ASAC Security Technology Subcommittee
- Keith Goll, TSA, Office of Requirements & Capabilities Analysis; Co-Chair, ASAC Security Technology Subcommittee

Security Technology Subcommittee Participants:
- Chris Bidwell, Airports Council International-North America
- David Borer, American Federation of Government Employees
- Colleen Chamberlain, American Association of Airport Executives
- Liam Connolly, Regional Airline Association
- Joe DePete, Air Line Pilots Association, International
- Ken Dunlap, Catalyst-Go Consulting, ASAC Vice-Chairman
- Loraine Howerton, United States Travel Association
- Susan Presti, The International Air Cargo Association
- Eric Thacker, Airlines for America
- Dean Walter, TSA

Subject Matter Experts:
- Dave Atkinson, Explosives Detection, Pacific Northwest Labs
- Jose Bonilla, TSA
- Anne Cowan, TSA
- Andrew Cox, Systems Analysis, Sandia National Labs
- John Fortune, Ph.D., DHS
- Jose Freig, American Airlines
- Matt Gilkeson, TSA
- Tim Harvey, TSA Technology Consultant
- Pete Hearding, TSA
- Andrew Karasick, TSA
- Janulyn Lennon, Hartsfield-Jackson Atlanta International Airport
- Mike McCormick, Global Business Travel Association
- John Clayton, McKinsey
- Andrew Meehan, Global Business Travel Association

- Kim Mills, U.S. Customs & Border Protection
- Ken Mortensen, former Associate Deputy Attorney General, Privacy & Civil Liberties, Department of Justice; former Deputy Chief Privacy Officer, Department of Homeland Security
- Jeffery Oboy, M2P Consulting, Inc.
- Patricia Rojas-Ungar, United States Travel Association
- Antoine Rostworowski, ACI World
- Colin Soutar, Deloitte
- Adam Steffl, Denver International Airport
- Jason Thorton, MIT Lincoln Laboratory
- Sterling Wiggins, TSA
- Mara Winn, TSA
- Terrence Young, Gensler