Risk-Based Security and the Aviation System: Operational Objectives and Policy Challenges

Issue Brief # 2015-02

Christian Beckner

Deputy Director,
GW Center for Cyber & Homeland Security

Center for Cyber
& Homeland Security

THE GEORGE WASHINGTON UNIVERSITY

I. INTRODUCTION

Risk-based security has been the primary strategic imperative for the Transportation Security Administration (TSA) for the past three and a half years, as a focused effort to move beyond a one-size-fits-all approach to aviation security and carry out TSA's mission in a way that is more efficient and improves the public perception of the passenger screening system without diminishing overall security.

The signature program of TSA's risk-based security strategy is PreCheck (written as Pre ✓™ in TSA literature), a voluntary program for expedited security screening of vetted low-risk passengers, based either on their direct application to the PreCheck program or a related program (such as Customs and Border Protection's Global Entry program); or on their status (for example, as a high-level member of an airline's frequent flier program or as an active duty member of the U.S. Armed Forces). PreCheck has been a significant success story for TSA since its launch in 2011, leading to a streamlined passenger screening process for millions of travelers and saving TSA in the range of $100 million in the last fiscal year, with operational savings and cost avoidances likely to continue to increase as the program further expands.

The rapid early growth of PreCheck has undoubtedly been a success story for TSA, one that has improved the agency's image with Congress and with the general public. As recently retired TSA Administrator John Pistole noted in prepared remarks for an October 2014 speech:

> *"What began as a proof-of-concept at just a handful of airports in 2012 has grown to include 120 airports and millions of travelers. From an innovation standpoint, TSA Pre✓™ represented a fundamental shift in our screening operations, and has proven to be quite a success."[1]*

But as the PreCheck program matures, it now finds itself at a critical decision point. Does it continue to grow incrementally within the scope of its current operational construct? Or does it seek a much greater growth trajectory,

---

[1] John S. Pistole, Transportation Security Administration. Prepared Remarks at ICAO Symposium on Innovation in Aviation Security. October 21, 2014. Available at http://www.tsa.gov/press/speeches/remarks-tsa-administrator-john-s-pistole-icao-symposium-innovation-aviation-security

including by enlisting the private sector to support enrollment efforts?   At what point does the expansion of PreCheck reach the point of diminishing returns, both in terms of security and operational efficiency? What are the benefits and risks of incremental growth vs. broad expansion of PreCheck with respect to aviation security generally? And what lessons can we learn from previous efforts at TSA to establish risk assessment and trusted traveler programs for aviation security?

This paper looks first at the history of risk-based passenger screening activities within TSA since its founding, including earlier TSA programs such as CAPPS II and Registered Traveler. It then provides an overview of the risk-based security concept and the development of PreCheck within TSA over the past four years, and looks at the benefits to date from the program. The paper then examines prospects for future growth within PreCheck, including assessing the current proposal to establish a private sector vetting initiative that would provide new private sector-led enrollment mechanisms for the program. Finally, the paper makes a few high-level observations about the long-term future of risk-based security and PreCheck in light of evolving threats to the aviation system, and concludes with a set of seven recommendations to TSA, the DHS Privacy Office, and Congress.

II. THE HISTORY OF RISK-BASED SECURITY WITHIN TSA

The policy basis for risk-based security activities within TSA was established at the agency's inception in the days and weeks after the terrorist attacks of September 11, 2001. The October 2001 report of the Secretary of Transportation's Rapid Response Team noted that there was "an urgent need to establish a voluntary means by which passengers might submit to an effective pre-screening regimen and thereby qualify for more expedited processing."[2] The Aviation and Transportation Security Act (ATSA), which established TSA and was signed into law in November 2001, included a provision for TSA to "establish requirements to implement trusted passenger programs and use available technologies to expedite the security screening of passengers who participate in such programs, thereby allowing security screening personnel to focus on those passengers who should be subject to more extensive screening."[3]

---

[2] "Meeting the Aircraft Security Challenge: Report of the Secretary's Rapid Response Team on Aircraft Security." October 1, 2001. Available at http://avalon.law.yale.edu/sept11/dot_010.asp
[3] Aviation and Transportation Security Act, P.L. 107-71. Section 109(a)(3).

For much of the first decade of TSA's existence, it struggled to fulfill this mandate to take a risk-based approach to passenger screening. TSA moved quickly after it was established to enhance IT systems to improve the pre-screening of passengers and to develop a trusted traveler program, but both of these efforts ran into serious roadblocks. These early experiences informed the development of the model for risk-based security activities at TSA, and also offer potential lessons today for the future of PreCheck.

Passenger Pre-Screening at TSA: The CAPPS II Experience

The Computer Assisted Passenger Prescreening System (CAPPS) was developed by the Federal Aviation Administration and U.S. airlines in the 1990s to provide a basis for risk-based screening of aviation passengers based on information in travelers' Passenger Name Record (PNR), including both biographical information and travel patterns determined to be suggestive of a higher degree of risk (such as the purchase of a one-way ticket). CAPPS was in operation on September 11, 2001 and seven of nineteen hijackers were flagged as selectees based on CAPPS, according to the 9/11 Commission.[4]

CAPPS II was announced by TSA in 2002 as an update to CAPPS that would be government-operated (unlike CAPPS) and that would draw on a much broader set of data – including both government data sets and commercially available data – to establish risk-based scoring of airline passengers that would inform passenger and baggage screening operations prior to boarding.

The CAPPS II proposal quickly attracted a significant amount of concern among leading privacy and civil liberties organizations, particularly with respect to the scoring of travelers and the use of commercial data to support decision-making.[5] These concerns were heightened by reports that JetBlue had in 2002 provided millions of its travelers' records to a Department of Defense contractor that was working on a similar project to CAPPS II – a transfer of data that was in part facilitated by TSA.[6]

---

[4] 9/11 Commission, Staff Statement #3, "The Aviation Security System and the 9/11 Attacks." Available at http://govinfo.library.unt.edu/911/staff_statements/staff_statement_3.pdf
[5] See for example, Electronic Freedom Foundation, "Government Surveillance via Passenger Profiling", available at http://w2.eff.org/Privacy/cappsii/background.php; and American Civil Liberties Union, "Feature on CAPPS II", available at https://www.aclu.org/technology-and-liberty/feature-capps-ii
[6] See Department of Homeland Security Privacy Office, "Report to the Public on Events Surrounding the jetBlue Data Transfer", February 20, 2004. Available at https://www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_jetblue.pdf

CAPPS II also faced a number of system planning and development challenges. For example, as GAO noted in February 2004, DHS and TSA had not "determined and verified the accuracy of databases to be used by CAPPS II" and had not "stress tested and demonstrated the accuracy and effectiveness of all search tools to be used by CAPPS II."[7]   These controversies and challenges with implementation ultimately led TSA to pull the plug on CAPPS II in late 2004, and shift to a new program, Secure Flight, that would not use commercial data and would focus primarily on matching airline passengers against records from subsets of the Terrorist Screening Database (TSDB), such as the No-Fly List and Selectee List. Secure Flight became fully operational in 2009 and plays a significant role in informing TSA's risk-based security efforts today.

The Registered Traveler Program

TSA announced an additional new program in 2004, at around the same time that it was cancelling CAPPS II and initiating Secure Flight: the Registered Traveler program (RT), established pursuant to the requirements of Section 109(a)(3) of ATSA.[8]   The goal of Registered Traveler, as stated by TSA Administrator Kip Hawley in 2005, was to "conduct more extensive threat screening in advance of travel on individuals who choose to participate in the program, and to provide those who are accepted into the program with expedited screening at the airport."[9]

Registered Traveler expanded beyond the pilot project phase in 2005-2006, with a focus on enlisting private sector companies to develop and enroll people into registered traveler program and staff dedicated screening lanes for their program members.[10]   The most active company in this market was CLEAR, which grew quickly to establish operations at 20 airports and

---

[7] See U.S. General Accounting Office, "Aviation Security: Computer-Assisted Passenger Prescreening Program faces Significant Implementation Challenges." February 2004. Available at http://www.gao.gov/new.items/d04385.pdf

[8] Details on the initial vision for the Registered Traveler pilot are in the TSA's Privacy Impact Assessment for the program, June 24, 2004, available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_rt.pdf

[9] TSA Administrator Kip Hawley, Testimony before the House Committee on Homeland Security, Subcommittee on Economic Security, Infrastructure, Protection and Cybersecurity. November 3, 2005. Available at http://www.tsa.gov/sites/default/files/publications/pdf/testimony/110305_hawley.pdf

[10] Transportation Security Administration, "TSA Announces Key Elements of Registered Traveler Program", January 20, 2006. Available at http://www.tsa.gov/press/releases/2006/01/20/tsa-announces-key-elements-registered-traveler-program

enrolled more than 200,000 members, but suddenly went bankrupt in 2009, leading to an immediate cessation of its operations.[11] CLEAR has gradually re-established a presence at a handful of major airports in the years since its bankruptcy, but the future of private sector-run Registered Traveler programs remains uncertain in light of the competing value proposition of TSA PreCheck.

The Risk-Based Security Initiative at TSA

In June 2010, FBI Deputy Director John Pistole was confirmed to be the Administrator of TSA, and found himself leading an agency that had a poor public image, was having to adjust its screening activities to address a set of novel terrorist threats (most notably the liquid-based explosives threat to transatlantic flights from 2006, and the "underwear bomb" threat from the attempted attack on NWA 253 on Christmas Day, 2009), and was now for the first time operating in a constrained budgetary environment. TSA's risk-based security initiative was developed as an effort to address all three of these strategic challenges by fundamentally changing the agency's operational model for passenger screening.

The vision for TSA's risk-based security initiative and a cost-benefit analysis of it (versus other approaches) is discussed in detail in a 2011 Master's thesis by Ken Fletcher, who currently serves as Chief Risk Officer at TSA.[12]   In the thesis, Fletcher articulates how a program that segments travelers into four categories (trusted traveler, low risk, unknown risk, high risk) and establishes a sizeable population of trusted and low risk travelers by identifying known low-risk populations and using voluntary enrollment mechanisms can focus its screening resources on passengers posing an unknown or high risk, in a way that both improves security and creates operational efficiencies.

TSA has implemented PreCheck in the past four years in a way that is generally consistent with this approach. At the program's inception in 2011, it was focused on offering access to PreCheck lanes at selected airports to high-level members of major airlines' frequent flier programs. The program expanded to allow enrollees of U.S. Customs and Border Protection's trusted

---

[11] See Wall Street Journal, "Un-Clear: Registered Traveler Company Shuts Down", June 22, 2009. Available at http://blogs.wsj.com/middleseat/2009/06/22/un-clear-registered-traveler-company-shuts-down/
[12] Kenneth C. Fletcher, "Aviation Security: A Case for Risk-Based Passenger Screening." Naval Postgraduate School Master's Thesis, December 2011. Available at https://www.hsdl.org/?view&did=699603

traveler programs (such as Global Entry) to receive reciprocal access to PreCheck and to include active duty military service members.[13] Beginning in 2013, TSA launched a direct enrollment process for PreCheck, which has enrolled more than 800,000 people to date.[14] TSA also now uses its Risk Assessment program and a "managed inclusion" process to bring additional travelers into PreCheck lanes, based either on the results of Secure Flight checks prior to check-in or at the discretion of Transportation Security Officers while travelers are queuing at checkpoints, in part based upon how busy the PreCheck lanes are relative to the regular screening lanes. As GAO noted in a recent report, the implementation of this Risk Assessment system and the expansion of managed inclusion led to a sudden 300% increase in PreCheck utilization in October 2013.[15]

As a cumulative result of all of these efforts, currently around 45% of air travelers in the United States (more than 276 million in 2014) are receiving expedited screening.[16] This growth in PreCheck has allowed TSA to reduce its screener workforce, and the agency has estimated that these staffing efficiencies will allow it to save at least $100 million in the current fiscal year.[17] Public sentiment toward TSA appears to be improving as a result of PreCheck, in comparison with the period in 2010-2011 when body scanners were in their initial period of deployment at checkpoints, although authoritative polling has yet to be done to substantiate that impression.

III. THE FUTURE OF RISK-BASED SECURITY AND PRECHECK

PreCheck has been an unambiguous success to date for TSA, allowing it to enhance security and operational efficiency while at the same time reducing costs. However, the program currently finds itself at a critical decision point. It has likely already enrolled many of the high-frequency travelers and other

---

[13] Additional details on eligible populations are available at this link on the TSA website: http://www.tsa.gov/tsa-precheck/participation-tsa-precheck

[14] Announcement of direct enrollment program at http://www.tsa.gov/press/releases/2013/07/19/tsa-launch-application-program-tsa-precheck. Current statistics on enrollees (as of January 2015) at http://blog.tsa.gov/2015/01/reflections-on-risk-based-security-in.html

[15] See chart on page 17 of report by Government Accountability Office, "Aviation Security: Rapid Growth in Expedited Passenger Screening Highlights Need to Plan Effective Security Assessments." Report available at http://www.gao.gov/products/GAO-15-150

[16] Statistics on utilization of PreCheck lanes from http://www.nytimes.com/2014/12/02/business/considering-the-year-in-airport-security-with-the-tsa-chief.html and http://blog.tsa.gov/2015/01/reflections-on-risk-based-security-in.html

[17] Information on staffing efficiencies and savings from http://www.npr.org/2014/12/18/371597750/tsa-administrator-john-pistole-to-leave-at-month-s-end

"early adopters" via airline frequent flier programs, CBP's trusted traveler programs (which had approximately 2.5 million enrollees as of mid-2014)[18], and direct PreCheck enrollment. Beyond U.S. military service members and Department of Defense civilians (which have already been added to PreCheck), any new groups or categories of already-vetted individuals are likely to be relatively small as a share of air travelers.

PreCheck enrollment is likely to continue to grow at a gradual rate in its current form, but it remains highly reliant on its Risk Assessment program and managed inclusion to achieve its current level of participation. These non-enrollee programs are a mixed blessing for PreCheck and TSA. On the one hand, they fill the PreCheck lanes and help to promote the PreCheck screening experience, prompting people to want to enroll directly. On the other hand, they may serve as a deterrent to future PreCheck enrollment, if travelers find either that they can often get the PreCheck benefit for free, or if PreCheck lanes fill up with non-enrolled travelers and end up being not significantly faster than normal screening lanes.[19]

In addition, TSA receives no direct financial benefit for non-enrolled PreCheck travelers. Individuals who directly enroll in PreCheck currently pay $85 to apply for a membership that has a five year period of validity, funds which help to offset TSA's costs associated with the development of the program.

Options for Expansion and the Private Sector Vetting Initiative

As a result of this dilemma, TSA has been looking to aggressively expand the enrolled base of PreCheck members via new means of outreach and enrollment.   TSA first signaled its interest in this issue when it issued a Request for Information (RFI) in January 2013 on Third Party Prescreening, intended to "determine the feasibility of commercial solutions to accurately assess risk to the transportation system and to pre-screen passengers at a high degree of confidence in order to increase expedited physical screening."[20]

---

[18] Enrollment count for CBP trusted traveler programs cited in Government Accountability Office, "Trusted Travelers: Programs Provide Benefits, but Enrollment Processes Could Be Strengthened." May 30, 2014. Available at http://www.gao.gov/products/GAO-14-483.

[19] This dynamic is discussed in this recent news article: http://www.smartertravel.com/blogs/today-in-travel/tsa-to-flyers-say-goodbye-to-free-speedy-security-lines.html?id=19530559

[20] Industry Day II Presentation for TSA Third Party Pre-Screening RFI, February 28 2013. Available at https://www.fbo.gov/index?s=opportunity&mode=form&id=f103493ce458c58a982c8e3405f02ba2&tab=core&_cview=1

TSA used the RFI to solicit white papers from industry and carry out initial testing and evaluation of the responses it received, but decided in March 2014 to not move forward with live prototyping of potential commercial solutions as had been originally considered, instead deciding to work "with DHS Science and Technology Directorate in order to define standards for future third party solution applications."[21] The DHS Science and Technology Directorate's primary advisory committee, the Homeland Security Science and Technology Advisory Committee (HSSTAC) convened a "Third-Party Pre-Screening Task Force" in July 2013 as part of this follow-on effort.[22]

A year and a half after the conclusion of this RFI process, this issue became a renewed area of focus for TSA in September 2014, when Administrator Pistole announced that the agency would be establishing a new private sector vetting initiative:

> *"TSA is working to establish a relationship with the private sector to enhance its continued efforts to expand the population of travelers using TSA Pre✓™. By leveraging private-sector best practices in business operations, marketing, and algorithm optimization, TSA hopes to provide a better travel experience for an increased number of 'trusted travelers' while focusing our attention on unknown and potentially higher-risk passengers."*[23]

TSA provided more details about its plans for this private sector vetting initiative in recent Federal Register notices and publicly available acquisition documents.[24]   TSA's Statement of Work notes that the agency is requesting "ready-to-market solutions to add private sector application capabilities for the TSA Pre✓® program to increase the public's enrollment access…" The document describes the role that these private sector entities would play, including to "provide convenient and secure enrollment options and perform pre-screening of applicants to include identity validation, a criminal history

---

[21] Amendment 0006 to TSA Third Party Screening RFI, March 4, 2014. Available at https://www.fbo.gov/index?s=opportunity&mode=form&id=f103493ce458c58a982c8e3405f02ba2&tab=core&_cview=1

[22] HSSTAC Meeting Minutes, April 7-8, 2014, Page 12. Available at http://www.dhs.gov/sites/default/files/publications/HSSTAC-April-2014-Meeting-Minutes-508_0.pdf

[23] TSA Press Release, September 26, 2014, available at http://www.tsa.gov/press/news/2014/09/26/tsa-precheck-private-sector-vetting-initiative

[24] For Federal Register notices, see for example the docket folder "TSA Pre✓® Application Program; Expansion of Enrollment Options" available at http://www.regulations.gov/#!docketDetail;D=TSA-2014-0001. For relevant acquisition documents, see TSA Solicitation # HSTS02-15-R-OIA037, "TSA Pre Check® Application Expansion", available at http://www.fbo.gov.

records check and any additional approved, provisional, low-risk assessments."[25]

The document goes on to note that "TSA may also consider approving an option to use additional private sector processes to conduct a provisional risk assessment (based on an algorithm developed by the Contractor) for the purposes of assisting in identifying those individuals believed to pose a low risk to transportation security."[26] The paragraph then clarifies the categories of information that cannot be used as part of such a risk assessment, and that any algorithms must receive the prior approval of DHS before being used. If enrollees were preliminarily approved for PreCheck by the private sector entity, their application would be forwarded to TSA for a further round of vetting.

This proposal to establish a private sector vetting initiative would potentially increase the growth in paid enrollments for PreCheck, but in doing so it potentially creates three significant new risks for the program as a whole:

1. The use of the private sector intermediaries to handle enrollment and conduct vetting is reminiscent of the CAPPS II experience discussed earlier in the paper, and creates a number of new privacy-related risks. This is partially mitigated by the fact that PreCheck is voluntary and that TSA has limited the scope of information that private entities can use to carry out risk assessments. But there are still inherent risks associated with the private sector carrying out such vetting on behalf of the government, including due to the prevalence of erroneous information in many commercial databases, and the use of intermediaries creates new risks related to data breaches and/or the deliberate misuse of personal information. In addition, were a private sector company to go bankrupt or cease operations, as was the case with the Registered Traveler program, there would be issues to address with respect to enrollees' personal data.

2. The use of multiple private sector entities for PreCheck enrollment has the potential to create new security vulnerabilities for the program. It is unclear what types of information that companies would be able to use to authenticate applicants and carry out an initial risk assessment. While there will still be a secondary government role in vetting applicants after

---

[25] Statement of Work, TSA Pre Check;® Application Expansion, available at http://www.fbo.gov.
[26] Ibid.

this initial private sector risk assessment and screening is done, there are risks that this process will be less robust than the current process in terms of authenticating applicants and vetting them from a security standpoint.

3. The use of private sector vetting threatens to undermine the business case for TSA's direct PreCheck application process. In setting the fee for PreCheck in 2013, TSA assumed that it would have an average of 390,000 direct enrollees per year over the next five years.[27] If these private sector entities attract a significant share of enrollees who would have otherwise directly enrolled, that will potentially reduce direct enrollees and reduce TSA's expected fee revenue, although such losses will be partially offset by efficiencies gains due to a larger enrolled population in PreCheck.

Given these risks, it is essential that TSA move forward cautiously with any plans to alter the current model of PreCheck enrollment, and understand the potential long-term risks and consequences of private sector vetting on its current operational model and on the PreCheck program as a whole. If not implemented carefully, the private sector vetting initiative could lead to privacy violations or security shortfalls that in a worst case scenario could undermine the entire PreCheck program.

IV. LONGER-TERM CONSIDERATIONS

The evolution of aviation security in the United States in the 13 ½ years since the terrorist attacks of September 11, 2001 has been one of frequent shifts in strategy and operational protocols, often reactive in nature to the latest terrorist threat. The development of TSA's risk-based security initiative has been an effort to move beyond this cycle of novel threats and detection-focused countermeasures, and establish instead a risk-informed and intelligence-driven process that still looks at what is being brought onto the plane but increases the emphasis on identifying and scrutinizing unknown or high-risk travelers.

This new risk-based security model has been a success to date, but we know from the experience of the past decade that terrorist adversaries are constantly looking for weaknesses in the aviation security system, and will likely attempt

---

[27] See Transportation Security Administration, Pre ✓™ Application Program Fee Development Report, October 25, 2013. Available at
https://www.tsa.gov/sites/default/files/publications/pdf/stakeholders_PDF/fee_development_report_-_final_11_19_13.pdf

to exploit any gaps or weaknesses in PreCheck. For that reason, TSA needs to be active in anticipating such vulnerabilities, and needs to carefully temper its desire to expand the enrolled base of the PreCheck program with a degree of caution. If a terrorist were to successfully exploit PreCheck and carry out an attack on the U.S commercial aviation system, there is a strong likelihood of a counter-reaction that would halt or substantially diminish the program as a whole for years to come. That would be an unfortunate outcome, given the good work that has been done over the past four years to build PreCheck to the point where it is today.

Beyond these security concerns, TSA also needs to clarify what it sees as the optimal size of the enrolled or pre-cleared population for PreCheck from an operational standpoint. At a certain point, there will be diminishing returns in terms of operational efficiency from increasing enrollment, particularly among the segment of air travelers that utilize small to medium-sized airports where there may only be one or two screening lanes at the checkpoint.

V. RECOMMENDATIONS

On the basis of the discussion and analysis above, this report makes the following seven recommendations, five of which apply to the executive branch, and two to Congress:

1. TSA needs to engage in a broader public dialogue with a variety of stakeholders about its plans for expanding PreCheck in advance of any major decision to change the operational framework of the program, particularly with respect to initiating new mechanisms for enrollment and vetting by the private sector.

2. TSA should utilize its internal Red Team capabilities (or similar capabilities in other agencies or the private sector) to assess potential vulnerabilities with respect to its proposed plans for expanding PreCheck, and attempt to address and mitigate any vulnerabilities prior to moving forward with private sector enrollment and vetting.[28]

---

[28] TSA Red Team capabilities are described in a 2008 Government Accountability Office report, "Transportation Security: TSA Has Developed a Risk-Based Covert Testing Program, but Could Better Mitigate Aviation Security Vulnerabilities Identified Through Covert Tests." Available at http://www.gao.gov/new.items/d08958.pdf

3. To increase public confidence in PreCheck expansion plans, TSA and the DHS Science and Technology Directorate (including its HSSTAC advisory committee) should release additional public information about the Science and Technology Directorate's reviews in 2013-14 of third-party pre-screening, and minimize the use of the Sensitive Security Information (SSI) designation in doing so.

4. The Privacy Office at the Department of Homeland Security needs to develop and publish an updated privacy impact assessment of PreCheck and work with TSA to develop and clarify guidelines for the appropriate role of the private sector in carrying out vetting to support the program.

5. The TSA Office of Intelligence and Analysis, working together with the DHS Office of Intelligence and Analysis, the FBI, and other intelligence agencies, should develop and prepare a classified risk assessment on PreCheck expansion, and share that assessment with the committees of Congress that have jurisdiction over TSA.

6. Congress should continue to conduct robust and informed oversight with respect to PreCheck, including closely examining the private sector vetting initiative that is currently proposed.

7. Congress should request that the Government Accountability Office (GAO) carry out a study, building on its December 2014 study of PreCheck and other work that it has done within the past three years, and assess the potential benefits and risks of new plans for PreCheck expansion, including the private sector vetting initiative.[29]

---

[29] See Government Accountability Office, "Aviation Security: Rapid Growth in Expedited Passenger Screening Highlights Need to Plan Effective Security Assessments." December 2014. Available at http://www.gao.gov/products/GAO-15-150

ADDITIONAL WORKS CONSULTED

The following reports were consulted in the development of this report, in addition to those reports previously cited in the footnotes:

Air Line Pilots Association, International. "Meeting Today's Aviation Security Needs: A Call to Action for a Trust-Based Security System." January 19, 2010. http://www.alpa.org/portals/alpa/pressroom/pressreleases/2010/whitepapers/aviationsecurit ysystemwp_1-19-10.pdf

Bossert, Thomas P. "TSA Compromising Security for Popularity; and Looking at our Credit Purchases?" *The Hill*, January 14, 2015. http://thehill.com/blogs/congress-blog/homeland-security/229406-tsa-compromising-security-for-popularity-and-looking-at

Elias, Bart. "Risk-Based Approaches to Airline Passenger Screening." Congressional Research Service Report, March 31, 2014. https://www.hsdl.org/?view&did=752251

Jackson, Brian A., Edward W. Chan, and Tom LaTourrette. "Assessing the Security Benefits of a Trusted Traveler Program in the Presence of Attempted Attacker Exploitation and Compromise." RAND Working Paper, May 2011. Available at http://www.rand.org/content/dam/rand/pubs/working_papers/2011/RAND_WR855.pdf.

Martonosi, Susan Elizabeth. *An Operations Research Approach to Aviation Security*. Thesis (Ph.D.). Sloan School of Management, Massachusetts Institute of Technology, 2005. http://dspace.mit.edu/handle/1721.1/33671

Transportation Security Administration, "Risk-Based Security Overview" (presentation). September 16, 2014. http://www.sgtp.org/Resources/Documents/EdCon'14%20TSA%20Risk%20Based%20Pre sentation.pdf

Transportation Security Administration, "Testimony of Steve Sadler before the House Committee on Homeland Security, Subcommittee on Transportation Security." September 18, 2014. http://www.tsa.gov/sites/default/files/publications/pdf/tsa_sadler_secureflightstatement.pdf

ABOUT THE AUTHOR

Christian Beckner is the Deputy Director of the Center for Cyber and Homeland Security (CCHS) at the George Washington University. Prior to the establishment of CCHS in January 2015, he served in a similar position on the staff of the Homeland Security Policy Institute and the GW Cybersecurity Initiative.

Before joining the George Washington University in early 2013, he served as an Associate Staff Director with the Senate Homeland Security and Governmental Affairs Committee, working for its Chairman, Sen. Joseph I. Lieberman, where he was responsible for coordinating the Committee's oversight of a wide range of homeland security and counterterrorism issues. His full biography is available at this link: http://cchs.gwu.edu/christian-j-beckner.

ABOUT THE CENTER FOR CYBER AND HOMELAND SECURITY

The Center for Cyber and Homeland Security (CCHS) at the George Washington University is a nonpartisan "think and do" tank whose mission is to carry out policy-relevant research and analysis on homeland security, counterterrorism, and cybersecurity issues. By convening domestic and international policymakers and practitioners at all levels of government, the private and non-profit sectors, and academia, CCHS develops innovative strategies to address and confront current and future threats. CCHS was established in early 2015 and integrates the activities and personnel of the Homeland Security Policy Institute (HSPI) and the GW Cybersecurity Initiative.