



white paper

Risk Management in a Volatile World: Preserving Visa Waiver Programs in the Era of International Terrorism

Mark Cohn, Vice President and Chief Architect

strategies

Introduction.

Today, many countries have established programs that permit people to travel to those countries without visas. Traveling under these visa waiver programs is very convenient, as a traveler often needs only a valid passport. By contrast, if a visa is required, a traveler may need to visit the destination country's consulate, submit to an interview, provide detailed background and travel information, furnish a biometric (e.g., a digital photograph or a set of fingerprints), undergo a security screening, and then await notification whether the visa will be issued or denied.

In the era of international terrorism, visa waiver programs pose significant security challenges because there is little or no security screening performed before travel. As a result, people on watchlists or engaged in terrorist or criminal activities may be able to board an aircraft and travel with relative ease. This creates obvious aviation security threats and may contribute to the ability of terrorist organizations to establish cells, conduct meetings and perform surveillance.

The security challenges posed by visa waiver programs should be of great concern to all governments. In the United States, for example, not only did Richard Reid (the so-called "shoe bomber") and Zacarias Moussaoui travel to the United States from visa waiver countries, but the horrific attacks in Madrid and London have underscored that there are sophisticated terrorist networks operating in Europe whose members may travel to the United States without visas. Conversely, countries in Europe may be concerned with travelers from North America because terrorists have traveled outside of North America for planning and training purposes (e.g., Mohammed Atta and members of the so-called "Lackawanna Six"). And many countries should be concerned with the presence of al Qaeda and related organizations, such as Jamaah Islamiah, in countries outside of Europe and North America that are afforded visa waiver privileges.

To mitigate their vulnerability, countries with visa waiver programs have two options: (1) eliminate such programs; or (2) enhance the security of visa waiver travel. The first option is unappealing because visa waiver travel fosters international commerce, tourism and cultural ties among

nations. Indeed, for these reasons and perhaps others, the G-8 recently reaffirmed its commitment to "visa-free" travel when launching the "Secure and Facilitated International Travel Initiative" (SAFTI) at its 2004 summit.

Thus, governments should pursue the second option — strengthening the security of visa waiver travel. This process is underway. The SAFTI, for example, commits the G-8 nations to developing interoperable electronic passports with advanced security features (e-passports), strengthening passport issuance standards, sharing information on lost and stolen passports and exchanging terrorist watchlist data. But these efforts are incomplete in scope and so far are only in their nascent stages. A more comprehensive approach to enhancing the security of visa waiver travel would: (1) identify the key facets of the visa issuance process that provide security; and (2) implement process, policy and technology changes that would replicate these features (to the extent practicable) without compromising the fundamental feature of visa waiver travel — the speed and convenience associated with traveling carrying only a passport. The remainder of this Paper examines potential changes to visa waiver programs based on the application of these principles.

The Security Features of Visa Travel.

The visa issuance and travel process provides governments with numerous opportunities to identify and interdict terrorists. As the G-8 recognized in SAFTI, the security of visa and visa-free travel begins with the passport application. The government issuing the passport may, for example, collect biometric and other data to confirm an applicant's true identity and to check that identity against domestic and international watchlists.

In a visa system, the destination country also may perform its own security screening, such as a watchlist check, based on biometric and other data collected as part of the visa application process. In addition, the biometric data collected from the visa applicant may be compared to the biometric data of the actual traveler, thereby preventing visa fraud. Finally, the visa issuance process provides the destination country with an opportunity to identify suspicious people through a face-to-face interview. The potential security benefits associated with visa travel,

therefore, are derived from three principal controls: (1) performing security screening before travel; (2) collecting biometric data and verifying identity; and (3) and conducting face-to-face interviews.

Notwithstanding significant differences between visa and visa waiver travel, these three controls could be integrated into visa waiver systems without substantially disrupting international travel. Indeed, some of the concepts underlying these controls already have been incorporated into international travel and visa waiver systems.

Securing Visa Waiver Travel.

Screening Travelers before Departure

The Vision

A security screening process for visa waiver travelers should have three components. First, each traveler should be checked against the various watchlists maintained by the destination country (e.g., lists of known or suspected terrorists and “no fly” lists). In addition, each traveler should be checked against the watchlists maintained by the country issuing the passport as well as other international watchlists. This is particularly important if the country issuing the passport does not include such checks as part of its passport issuance process or if its legal system does not permit the government to deny passports to suspected terrorists.

Second, each traveler should be screened for indicia of suspicious behavior or inadmissibility. Such a screening process should, among other things, compare the traveler’s passport number(s) to a current listing of lost and stolen passports from visa waiver countries. As the G-8 and the Inspector General in the United States Department of Homeland Security have recognized, such a screening system must be developed because passports from visa waiver countries are frequently stolen and used by transnational criminals in order to avoid the scrutiny applied to visa applicants.

Third, the screening process should be completed in advance of aircraft boarding so that the destination country could issue a board or no board instruction to airlines with respect to each passenger. Indeed, establishing such a

system is essential to addressing the vulnerabilities inherent in visa waiver programs.

Depending on the type of screening performed, the destination country’s decision to deny a person from boarding an aircraft could be based on national security grounds or the discovery of information demonstrating that the traveler is otherwise inadmissible (e.g., previous visa overstay). An airline, however, need not be informed of the basis for a board/no board decision. Indeed, by issuing a generic instruction not to board a particular passenger, a destination country may be able to better preserve the integrity of its watchlists. Under such circumstances, both the airline and the traveler would be unable to determine if the denial were based on national security or admissibility considerations.

The Landscape

With the exception of Australia, no country permitting visa waiver travel has developed a system for the routine screening of passengers before boarding. In Australia, the government obtains passport and other data at the time an airline reservation is made. The government uses this information to screen travelers using several criteria, and those who are approved for visa-free travel are issued an Electronic Travel Authorization (ETA) well in advance of foreign departure.

Although no country has followed Australia’s lead, the hurdles to implementing a pre-boarding screening system are relatively modest. The data and technology required to screen visa waiver travelers already exist. Moreover, depending on the amount and types of information required by the destination country, the procedures for making boarding decisions and communicating them to airlines may be implemented with relatively modest changes in business practices.

The data that a destination country needs to screen visa waiver travelers — such as name, date of birth, citizenship, passport number and travel itinerary — are currently captured through a variety of commercial and government records and electronic systems. Information regarding a person’s identity, for example, is captured in print and in the Machine Readable Zone (MRZ) of a passport. In addition, travel and itinerary information — so

called Passenger Name Record (PNR) data — is currently captured in airline reservation and departure control systems. Finally, other types of itinerary information, such as intended destination, may be captured on immigration forms (e.g., United States Form I-94).

The technology needed to share watchlists in a manner that is secure and consistent with data privacy requirements also exists and is widely available. In Chile, for example, immigration authorities collect biometric data on arriving travelers and compare that data to an Interpol watchlist in a rapid and reliable manner. The United States and Canada, moreover, are routinely exchanging watchlist data in an automated fashion for use by their respective customs and immigration authorities. Similarly, although efforts to establish a central Interpol clearinghouse for lost and stolen passport data are still underway, the automation technologies used to share watchlist data enable governments to share information on lost or stolen passports as well.

In light of the available data and proven information sharing technologies, several countries already screen arriving travelers on a post-departure basis. The United States and Canada, for example, require airlines to collect Advance Passenger Information (API) — principally MRZ passport data — on all passengers, and to transmit the API to the government shortly after takeoff. Both countries also review PNR data on arriving international air travelers. Together, the API and PNR data are used to check travelers against watchlists, and to identify suspicious behavior or indicia of inadmissibility.

The Path Forward

The types of screening systems developed by Australia, Canada and the United States could be adapted in a variety of ways to permit sophisticated pre-departure security screening without substantially disrupting airline operations. The key issues for a government developing such a system would include: defining the data that would be required before boarding (e.g., MRZ passport data, PNR data, destination and/or other types of data); identifying the methods for transferring that data (e.g., requiring airlines to provide that data and/or accessing airline reservation systems to obtain the data); determining how the data would be used (e.g., conducting watchlist checks and/or

data analysis to identify suspicious or inadmissible travelers); and establishing when the data would be transferred and the amount of time it would take to communicate boarding decisions to airlines (e.g., in seconds if a fully automated process or longer under some conditions).

The decisions made by governments, particularly with respect to required data and processing times, will determine the extent to which the screening process can be integrated into airline operations with little or no disruption or change in business processes. For example, if a government were to determine that it would require only MRZ passport data (and perhaps access to PNR data) for the purpose of performing pre-departure watchlist and stolen passport checks, then such a pre-departure screening system would require virtually no change in current airline operations. Just as they do today in many airports, airlines could swipe passports at the check-in counter (or at the transit counter or departure gate for connecting passengers) to transmit MRZ data (and permit governments to access PNR data in advance of departure). Using available processing technologies, a government could obtain this information, check it against various watchlists and databases, and via rapid communications convey a boarding decision to an airline in no more than a few seconds. As a result, the entire screening process could be integrated with normal check-in procedures with virtually no disruption to the boarding process.

By contrast, if a government were to determine that it would require pre-departure data from airlines that is not available in the MRZ of a passport, such as a traveler's destination address (which is currently required under United States law), then airlines would need to change their information systems and check-in practices to obtain this data by the time they capture and transmit MRZ passport data (i.e., check-in). Under such a system, airlines could require travel agents and on-line reservation systems to modify their systems and procedures to collect this information when a reservation is booked. In addition or alternatively, airlines could modify their check-in procedures to create a process to ensure that the necessary data is captured such as with the use of a self-service kiosk. Once collected, the required information could be linked to MRZ data and transmitted to a

government or made available to a government as an additional type of PNR data stored in an airline reservation system. The success of the ETA system in Australia suggests that these types of changes in business practices could be accommodated by the travel industry.

The most significant challenge to implementing a pre-departure screening system relates to the amount of time required by the destination country to make a boarding decision. If the screening process is longer than the normal check-in process, then airlines could be compelled to make substantial changes to their check-in and boarding procedures, such as establishing a two-step check-in process. The first step would take place before arriving at the check-in counter (or departure gate in the case of a connecting passenger) and would require a traveler to stop at a self-service kiosk to swipe his or her passport. He or she would then confirm the reservation (or purchase a ticket) and manually enter any non-MRZ data required by the destination country that is not already located in the airline reservation system. This information would then be transmitted (or made available) to the destination country, which would issue a boarding decision by the time the traveler arrived at the check-in counter (or departure gate) to obtain his boarding pass — the second step in the process.

Given the potential changes that could be required in airline passenger processing operations, governments establishing pre-departure screening systems should develop processes that minimize the amount of time required to make boarding decisions. As a practical matter, this may require countries to develop stringent criteria for when to instruct airlines not to board passengers and to implement other processes for resolving concerns about questionable travelers (e.g., performing a pre-departure interview or a secondary inspection upon arrival). But when coupled with current processing technologies, these business processes should enable countries to perform a range of automated security checks in a manner of seconds, thereby permitting the screening process to take place during normal airline check-in procedures.

Collecting Biometric Data and Verifying Identity.

The Vision

The biometric collection and identity verification process for visa waiver travelers should be designed to accomplish three security objectives. First, a biometric from the traveler should be obtained by the destination country and compared against available watchlists. This check is necessary to ensure that the true identity of the traveler is being checked against the appropriate lists.

Second, the biometric obtained from the traveler should be compared to the biometric embedded in the passport to ensure that there is a match — that the person identified in the passport is the actual traveler. This type of security check is necessary to combat document fraud, which is often associated with other types of illicit behavior.

Third, the biometric obtained from the traveler also should be compared to the biometric provided by the person who applied for the passport. This type of security check also is necessary to combat document fraud. There are sophisticated passport forgery and counterfeiting rings throughout the world that may be capable of creating a functioning false passport with a biometric that matches the bearer. Absent a comparison of the actual traveler to the biometric data on file with the issuing government, this type of document fraud may go undetected.

The Landscape

Today, no country that permits visa-free travel performs all of these three security controls. This is because no country other than Australia has issued a large number of so-called “e-passports” — passports with embedded biometrics. E-passports, however, will soon be commonplace. Not only will the United States soon start issuing e-passports, but all countries afforded visa waiver privileges by the United States must issue e-passports by October 26, 2006. In addition, according to ICAO, as many as 40 countries intend to issue e-passports in accordance with ICAO specifications within the next few years.

Conversely, the technology needed to incorporate digital photographs and biometric data into an identity verification process already exists. The United States and Chile, for

example, already compare such data against watchlists or biometric data stored in other databases. In Chile, immigration authorities use facial recognition and fingerprint matching technology to compare travelers against an Interpol watchlist. In the United States, fingerprints taken upon arrival as part of the US VISIT entry process are compared against various law enforcement databases. In addition, those fingerprints are also compared to the fingerprints provided by the visa applicant at the foreign consulate. Similarly, under the Registered Traveler program, the biometric provided by the traveler at an airport kiosk is compared to the biometric provided by the person who actually registered for the program. In each of these systems, the biometrics collection and database matching process has proven to be very efficient and reliable.

Similarly, the technology needed to quickly and reliably compare a biometric obtained from a traveler to a biometric embedded in a travel document also exists. This type of technology has been used in several countries, including Australia, which has integrated the verification of e-passport data into its arrival processes; the Netherlands, which has incorporated biometric verification in the Privium registered traveler program at Schipol airport; and Canada, which has used biometric verification as part of the CANPASS registered traveler program.

The Path Forward

Given the state of technology and the pending issuance of e-passports, it should not be difficult for countries permitting visa waiver travel to incorporate biometric collection and identity verification into normal border inspection processes. Indeed, the work done in Australia, Chile and the United States has demonstrated that border authorities can integrate biometric verification into normal airport operations with little or no disruption.

There will, however, be political and other challenges associated with efforts to compare traveler biometric data with the biometric data provided to the government issuing the passport. Not only will this type of data sharing potentially require new international agreements, but those agreements may be difficult to obtain in light of the varying data privacy regimes in place in countries that participate in visa waiver programs. Moreover, once those agreements are reached, the technology and business processes

needed to implement their terms could be complex, as there may be varying requirements for access controls, data retention and data sharing.

Another challenge facing countries permitting visa waiver travel will be whether to perform the biometric verification when a traveler arrives in the destination country (as is currently the norm for countries using biometric verification systems) or before a traveler boards a flight at a foreign airport. The latter approach would provide greater security by enhancing other screening efforts designed to prevent potential threats from boarding aircraft. It also would have economic benefits for the airlines because when a destination country is able to identify travelers carrying false documents before departure, the airlines can avoid the fines that are often imposed for carrying such inadmissible travelers.

The potential advantages of pre-departure biometric collection and identity verification, however, must be weighed against the potential costs and operational challenges associated with implementing such a system. The destination country could, for example, station its immigration officers in foreign airports to collect biometrics and verify identity. There is some precedent for this type of model, as the United States has stationed dozens of officers in Canadian and Caribbean airports to perform virtually all inspection functions under so-called “preclearance” agreements. But preclearance operations may not be attractive to the destination country because of the high costs associated with stationing officers overseas and questions about the legal authorities and immunities that such officers would possess. Similarly, the departure country may not find this model appealing because of the costs associated with reconfiguring airports and assigning government personnel to support the preclearance operation.

In the alternative, the departure country could station government personnel in its airports to collect biometrics and verify identity. This option may not be attractive to the destination country because its immigration authorities would not participate in the security control. And the departure country may find this option unappealing because of the legal questions and costs associated with performing these functions.

Finally, the airlines could perform the function of collecting biometric data and verifying identity during the normal check-in process. Assuming the cooperation of the destination country and the passport issuing country, the process of comparing the traveler's biometric to watchlists, the biometric embedded in the passport, and the biometric collected by the country issuing the passport could be performed in a few seconds using existing technologies. But such a model also may be unappealing to the destination country because that country may insist that these types of security controls be performed by its immigration authorities.

In light of the challenges associated with collecting biometrics and verifying identity before departure, countries permitting visa waiver travel should, at a minimum, integrate these security controls into their immigration inspection processes for arriving international air passengers as e-passports become more common. Visa waiver countries should also develop the agreements and systems necessary to permit a destination country to compare a traveler to the biometric collected by the passport issuing country. These enhancements would provide a meaningful increase in the security of visa waiver travel without diminishing its convenience. At the same time, visa waiver countries should develop and test options for collecting biometrics and verifying identity on a pre-departure basis to determine the viability of this potential security control.

Observing and Interviewing Visa Waiver Travelers

The Vision

A destination country should deploy relatively modest numbers of immigration officers to foreign airports to observe and interview suspicious visa waiver travelers before boarding. Such travelers could be identified through an automated screening process (e.g., travelers identified as suspicious or potentially inadmissible, but not meeting the criteria for automatically preventing boarding), through biometric checks (including those unable or unwilling to provide a sample of sufficient quality for positive identification), or observation. Under this type of control, some travelers would be interviewed, but the vast majority would not. If an officer were to elicit grounds for deeming a traveler to be inadmissible, the airline would be notified immediately of that determination and instructed not to board the traveler. Thus, this type of security control would not substantially alter the character of visa waiver travel, nor would it entail the costs and other complexities associated with preclearance.

Incorporating an opportunity to observe and interview passengers in a visa waiver security regime is necessary because the other components of such a regime — comparing names and biometrics to watchlists, analyzing data to identify suspicious travelers, and verifying identity — all have limitations. Indeed, there is ample evidence that observing and questioning a traveler may be the only way to identify some potential terrorists. In the United States, for example, Ahmad Ressaam (the so-called “millennium bomber”) was detained after questioning by a Customs inspector; he did not appear on any watchlist. Similarly, the likely 20th hijacker in the September 11, 2001 attacks was denied entry into the United States after questioning by an Immigration inspector; he too did not appear on any watchlist. Other nations also recognize the value of conducting face-to-face interviews. The national airline of Israel, El Al, which is widely regarded as the world's safest carrier, spends substantial time observing and interviewing passengers before permitting them to board.

The Landscape

Unlike other proposed enhancements to visa waiver security, deploying immigration officers to foreign airports would not require significant investments in technology by governments or changes in business practices by airlines. Canada, for example, already has successfully deployed Migration Integrity Officers (MIOs) to foreign airports to work with airlines and foreign governments to identify travelers carrying false documents or who otherwise may be inadmissible. Today, Canada has 45 MIOs posted in 39 foreign airports, and these Officers have interdicted thousands of inadmissible travelers. Similarly, in the aftermath of September 11th, the United States Immigration and Naturalization Service temporarily deployed dozens of Immigration Control Officers (ICOs) to foreign airports. The ICOs functioned much like their Canadian counterparts and successfully interdicted thousands of inadmissible travelers.

The Path Forward

Following Canada's lead, countries with visa waiver programs should permanently deploy immigration officers to select foreign airports. These officers would function much like MIOs or ICOs, but with a greater emphasis on observing and questioning suspicious travelers.

In addition to the security benefits associated with observing and interviewing potentially suspicious travelers, there would be other benefits associated with posting immigration officers in foreign airports. To begin with, these personnel would work with the airlines to identify travelers carrying false documents, thereby reducing the fines paid by airlines for carrying inadmissible passengers. In addition, the immigration officers could work with the airlines to resolve potential watchlist matches. This would expedite and simplify the travel process for those who are incorrectly identified as potential matches. They also provide the means to implement a third decision path such as hold for examination instead of automatic no board when a person can't be cleared within a specific threshold for the response from the automated system. Further, the officers could work with the airlines to ensure the proper execution of a biometric collection and verification process. Thus, by posting immigration officers in foreign airports, destination countries could potentially shift the biometric collection and identity verification process from arrival to check-in.

Conclusion.

As they are currently configured, visa waiver programs entail substantial risks in the era of international terrorism. Although the G-8 has begun to address vulnerabilities in visa waiver travel, that effort is in its nascent stages and is not comprehensive in scope. A more comprehensive effort to enhance the security of visa waiver travel would focus on mirroring the key features of visa systems that enhance security — screening prospective travelers for risk, collecting biometric data to verify identity and conducting face-to-face interviews — without eliminating the convenience of visa waiver travel or substantially disrupting airline operations.

Within this framework, there are many options for improving security and they impose differing costs, technological challenges, political considerations, and business process changes for governments and airlines. As a result, countries permitting visa waiver travel may adopt different strategies for strengthening the security of their visa waiver programs.

Nonetheless, any strategy to secure visa waiver travel should, at a minimum, be based on the rapid implementation of three basic security controls. First, a country permitting visa waiver travel should require airlines to collect MRZ passport data at the ticket counter (or the transit counter or departure gate in the case of a connecting flight) for transmission to the government so that it could be compared against various watchlists and databases and a boarding decision can be transmitted to the airline. This type of limited automated screening could be performed without great cost to governments or airlines and could be integrated into normal airline check-in and boarding procedures. Second, a country permitting visa waiver travel should require visa-free travelers to use e-passports. It should collect biometric data from travelers upon arrival and compare that data against watchlists and the biometrics embedded in the e-passports. This type of security check also could be performed quickly and reliably during normal immigration processing. Third, a country permitting visa waiver travel should strategically deploy immigration officers to foreign airports to observe and interview suspicious travelers. This type of tailored deployment could be sustained without great cost and without disrupting airline operations or diminishing the convenience of visa-free travel.

About the author:

*Mark Cohn, Vice President and Chief Architect
Global Public Sector
Unisys Corporation*

Mark Cohn is the vice president and chief architect for Unisys Global Public Sector, where he is responsible for the vision and architecture for strategic security programs including sales and delivery in target accounts in all geographies. In addition, Mark is responsible for architectural support to strategic Global Public Sector engagements and for global solution visibility centers. He is located in Reston, Va.

Since joining Unisys in 1985, Mark has served successfully in a broad range of engineering and management positions. He has directed strategic initiatives related to biometrics, positive identification and access control, information sharing across enterprise boundaries, securing the IT infrastructure, defense intelligence, and counterintelligence. Most recently, he was technical advisor and executive of interest for Unisys with the DOD Counterintelligence Field Activity, program manager for the Transportation Security Administration Registered Traveler pilot program and principal architect for the Department of Homeland Security US-VISIT Exit system. Prior to that, Mark managed the transition to Unisys of IT Production Support at the Executive Office of the President and architected the technical solution for the TSA Information Technology Managed

Services contract, as well as several interagency law enforcement information sharing systems.

In 2001, Mark was chief architect for Unisys health care solutions. From 1997 through 2000, he was general manager of the architecture and software development practice of the U.S. Federal Government Group service delivery organization, where he had responsibility to manage programs from sales through delivery at eight departments or independent agencies and also directed Unisys e-government initiatives.

Mark is an expert in the design and implementation of trustworthy, highly available distributed systems. He started his career at Unisys as a senior systems programmer on fault-tolerant systems used for aviation infrastructure management and was the principal designer and chief engineer for nation-wide critical command and control capabilities essential to air traffic control that have proven to be among the most reliable systems ever put into operation.

Mark holds a bachelor's degree in behavioral and social sciences from the University of Maryland, and a master's degree in management information systems from American University.

Contributor:

This paper was prepared in collaboration with Brian C. Goebel of "The Sentinel HS Group, LLC."

For more information, please visit our Website at:
www.unisys.com/public_sector

Specifications are subject to change without notice.

© 2005 Unisys Corporation.

All rights reserved.

Unisys is a registered trademark of Unisys Corporation. All other brands or products referenced herein are acknowledged to be trademarks or registered trademarks of their respective holders.

Printed in U S America 10/05

3831 0322-000