

Testimony of Marc E. Frey, Ph.D.

Before the Committee on Homeland Security and Governmental Affairs

United States Senate

“Visa Waiver Program: Implications for U.S. National Security”

March 12, 2015

Thank you Chairman Johnson, Ranking Member Carper, and distinguished members of the Committee for this opportunity to testify on the Visa Waiver Program (VWP) and its implications for U.S. national security. My name is Marc Frey. I am a senior director at Steptoe & Johnson LLP, an international law firm. Prior to joining Steptoe I served in several positions at the Department of Homeland Security (DHS), including as Director of the Visa Waiver Program from 2007-2010. In that role I oversaw the successful effort to enhance the security of and expand the VWP and managed the security assessments of member countries.

This is a timely hearing. Following the terrorist attacks in Paris earlier this year commentators have speculated on the possibility of an attack on U.S. soil by terrorists possessing passports from France or other VWP countries. Many in the media and elsewhere labor under the misapprehension that security standards are looser for VWP travelers than for those traveling with a visa, and that this poses a threat to U.S. national security. Concerns have been raised, for example, about the ability of ISIS terrorists with “Western” passports to enter the United States under the VWP by circumventing the consular interview.

Under the VWP, DHS waives the “B” nonimmigrant visa requirement for aliens traveling from the 38 approved countries, permitting stays of up to 90 days for business or tourism. A consular interview is not required. But, that does *not* mean that DHS waives security requirements for these travelers. In fact, it mandates additional, more stringent security

requirements, for both the individual traveler and his or her home country. The result is a system that provides as much security against terrorist or criminal travelers as the visa system.

Like any successful security program, VWP has been closely reviewed over the years, undergoing reform and modernization as new threats arose. It's fitting, then, to discuss potential enhancements to the program in response to today's dynamic threat landscape. At a minimum, DHS must ensure that participating countries are fully meeting their information-sharing obligations. Other options to strengthen the program include steps that DHS can take unilaterally, such as adding new data fields to ESTA, as the Department did last year, or further tightening passport requirements. They also include measures that may require or benefit from legislative action, such as making a handful of discretionary considerations mandatory, upping the frequency of eligibility reviews, or requiring participating countries to screen travelers against databases, such as INTERPOL's Foreign Fighter database or its Stolen and Lost Travel Document database.

Evolution of the VWP

Since its inception in the late 1980s, the VWP has evolved into an essential tool for increasing global security standards, advancing information sharing, strengthening international relationships, and promoting legitimate trade and travel to the United States. Over the past decade in particular, Congress and the Executive branch have worked together to implement a number of enhancements to the VWP to address evolving threats to international travel and to the United States homeland. Therefore, although critics of the VWP often continue to cite the example of the "Shoe Bomber" Richard Reid, who as a British citizen traveled under the VWP in December 2001, the reforms put in place over the past dozen years have successfully addressed this risk to date.

For example, in 2003 new requirements were put in place to tighten passport security standards for VWP travelers and to increase the frequency with which countries are formally reviewed for their designation status. Furthermore, in order to align with the recommendations of the 9/11 Commission, Congress, in 2007, mandated additional security requirements to VWP, including standards for secure travel documents, individualized pre-screening of travelers, bilateral information-sharing arrangements, prompt reporting of lost and stolen passports, and a threat assessment conducted by the Director of National Intelligence. These reforms have made the VWP a significant, security-enhancing program and a critical element of the layered border security approach the U.S. has implemented since September 11, 2001.

Key Security Components of the VWP

As described below, the VWP enhances U.S. security in four mutually reinforcing ways:

- It enables individualized and recurrent screening of travelers against law enforcement and security databases;
- It mandates bilateral and multilateral information and intelligence sharing;
- It requires secure passports to confirm identity; and
- It permits regular audits of the security standards of participating countries.

First, the VWP screens all travelers against multiple law enforcement and security databases, including the Terrorist Screening Database, before they depart for the United States. Using the online Electronic System for Travel Authorization (ESTA), a VWP traveler is required to provide biographic information (including name, date of birth, and passport number) as well as his or her destination address in the United States. The traveler is also required to answer questions regarding communicable diseases, arrests, convictions for certain crimes, and past history of visa revocation or deportation. In November 2014, DHS expanded the personal data

required for an ESTA application, to include national identity numbers for those who have them and data from a second passport if that passport is not from a VWP country, among other data elements. As a result, ESTA functions as a powerful screening tool, enabling recurrent, individualized vetting of travelers. Travelers without an ESTA approval cannot board a flight to the United States.

Second, the VWP mandates robust information and intelligence sharing between the United States and its VWP partners, including agreements concerning known or potential terrorists and criminals and reporting lost and stolen passport (LASP) data to the United States. Supplementing the U.S. government's "watch lists" and other databases with these three pieces of information from a traveler's home government greatly enhances DHS's ability to identify and stop travelers who pose a threat.

Third, all VWP travelers must use secure travel documents that meet internationally recognized standards, which allows for easier detection of forged or fraudulent passports. The majority of VWP travelers are required to use electronic passports (e-passports), which have an embedded chip that includes the bearer's biometric information.¹ At the port of entry, the biographic and biometric data contained in the electronic chip is compared to both the traveler and the travel document being presented. There are many other layers of technical security in the e-passport production process and the document itself that make duplication or forgery much less likely.

Lastly, VWP countries are required to undergo periodic eligibility reviews designed to ensure that VWP membership does not compromise U.S. security, law enforcement, and immigration enforcement interests. These comprehensive assessments are conducted by DHS, with the

¹ All passports issued after October 26, 2006, presented by aliens entering under the VWP must be electronic passports.

assistance of other U.S. government agencies as appropriate. Critically, these reviews involve a site visit during which a team of U.S. government subject matter experts examines the country's security and law enforcement capabilities and procedures. Among other issues, a site visit focuses on the existence of radicalized groups in the country and the government's efforts to address this concern. The findings from the site visit form the core of the comprehensive DHS evaluation of a country's fitness to continue participating in the VWP. Should DHS identify any issues or concerns during the course of its review, it can propose and insist on mitigation measures.

To complement these reviews and to ensure recommended mitigation measures are carried out, DHS has developed a vigorous monitoring process to ensure awareness of changing conditions in VWP countries. This monitoring process includes regular consultation with U.S. law enforcement and intelligence agencies, as well as frequent communication with relevant U.S. Embassies abroad and foreign embassies in Washington for updates on law enforcement or security concerns related to the VWP. Overall, no other program provides the U.S. government with the opportunity to conduct as far-reaching and consequential audits of foreign security standards, ensuring alignment with our high standards for managing risk.

Under current law, DHS has the authority to immediately terminate a country's membership if an emergency occurs in the country that threatens the law enforcement or security interest of the United States. The Director of National Intelligence is also able to recommend immediate suspension to DHS if any current and credible threat poses an imminent danger to the United States or its citizens and originates from a country participating in the VWP.

That the modernized VWP enhances U.S. security is widely recognized by security experts across the political spectrum. The last three secretaries of homeland security, for example, have

praised the program's contribution to U.S. and international security. Indeed, for precisely that same reason, both the Bush and Obama administrations have added countries to the VWP. The VWP's security components make so much sense, in fact, that they are setting global standards for countering terrorist travel. A September 2014 UN Security Council Resolution on security measures to better track and deter terrorist travel activity reflects practices the VWP has enforced for member countries since 2008.

The VWP and U.S. Border Security

Because of its strong security components, the VWP has become an integral part of the U.S. government's ability to identify security or other risks associated with travelers at the earliest possible point and push-out our "virtual" border. In particular, the VWP helps answer the three key questions necessary to implement an effective risk-based screening system:

- "Who is a threat?" – U.S. officials need to identify known and suspected terrorists as well as other individuals who may pose a threat.
- "Is the person coming to the U.S.?" – U.S. officials need to know, as early as possible, if the traveler should be examined more closely.
- "Is the person really who he says he is?" – U.S. officials determine if the traveler is presenting fraudulent documents.

Who is a threat?

The U.S. government collects and maintains an array of information designed to identify those associated with terrorism or other illicit activities. These "watch lists" use identifiers – primarily biographic-based, but increasingly incorporating biometrics – to support border-screening protocols and procedures. However, when it comes to identifying dangerous individuals from abroad, the U.S. government is not the only, or necessarily the best, source of

information. In fact, if you wanted to identify potentially dangerous individuals from a particular country, say the UK, your first stop would not be Washington; it would be London. Many European countries have rapidly growing ethnic and religious immigrant communities, a small minority of which has the potential to become radicalized. It makes sense then that the person's home country is the best source of information about which of its citizens or residents is most likely to pose a risk to the United States. This kind of unprecedented bilateral and multilateral information sharing mandated by the VWP, along with the routine audits and inspections made possible by the program improves the U.S. government's overall ability to identify bad actors and activity.

Is the person coming to the U.S.?

DHS begins the screening process well before a potentially risky traveler reaches the U.S. border; in fact, DHS begins the process before the traveler even arrives at an airport through ESTA. In addition to the ESTA requirement for VWP travelers, DHS requires airlines to provide a copy of their passenger manifests and data from their reservation files. This information – which applies to all travelers and is provided to DHS a minimum of 72 hours in advance – helps the agency determine who to allow onboard a U.S.-bound plane, who requires further screening and investigation upon arrival, and who should be turned away and referred to appropriate law enforcement personnel. These advance-screening measures give DHS a better, more informed understanding of who is coming to the United States.

Is the person really who he says he is?

No amount of “watch listing” and passenger screening will detect terrorists if they are able to travel on an assumed identity with fraudulently obtained or fake documents. In order to verify that people are who they say they are when they travel, DHS insists on high standards for

documents acceptable for entry to the United States. These standards are highest for VWP travelers. For example, the electronic passports mandated by the VWP enable DHS to incorporate biometric verification—digital photographs and, increasingly, fingerprints—in the screening process to confirm that the person presenting the document is the person that the document describes. And, DHS routinely audits the document production and issuance process in VWP countries to ensure standards are being met. In other words, VWP makes it harder to enter the United States using fraudulent documents and forged identities.

These three elements – who’s risky, who’s coming here, and who’s who – work together both prior to take off and at the port of entry to help U.S. officials identify terrorists and criminals and prevent them from traveling here.

Strengthening the VWP

It is essential that we continually look to identify possible enhancements to the VWP in the face of current threats, much like DHS continually evaluates participating countries and recommends improvements to their security postures. As noted above, there are a number of sensible ways to strengthen the VWP, but any measure that would curtail the program even temporarily would be damaging and wrongheaded. Rather than enhance U.S. security, such a step would undermine it, resulting in the loss of significant leverage over the security standards of both current and prospective members, to say nothing of the severe economic and diplomatic consequences.

For current VWP members, suspension of the program would undermine current information and intelligence-sharing mechanisms and deprive the U.S. of visibility into their security practices, including those to prevent radicalization and identify foreign fighters. It would also

undermine relationships with our closest allies in the face of common threats ranging from ISIS to a resurgent Russia.

For prospective members, the disappearance of the program would remove a powerful and proven incentive to elevate security standards and to enhance cooperation with the United States on security matters. A number of countries, for example, have unilaterally upgraded to e-passports so as to be eligible for the VWP. Likewise, several prospective members have signed the information-sharing agreements and otherwise increased law enforcement and security-related cooperation with the United States in the hopes of meeting the program's requirements. These actions provide tangible security benefits to the United States and to the international travelling public well in advance of potential VWP designation.

While emotional responses often occur in times of heightened security concerns, any discussion of the VWP and national security must remain focused on the facts. And the facts are that the VWP has proven to be an effective leverage point for raising and maintaining security standards while providing unprecedented levels of information sharing and access, allowing the United States to better manage risk. The program not only has improved overall U.S. security, but it has also facilitated the flow of lawful travel.

Again, thank you for inviting me to testify today. I look forward to answering any questions the committee may have.