Testimony of C. Stewart Verdery Jr.
Assistant Secretary for Border and Transportation Security Policy and Planning
Department of Homeland Security
Senate Committee on Foreign Relations
Sub-Committee on European Relations
May 13, 2004

Chairman Allen, Ranking Member Biden, and Members of the Committee, thank you for the invitation to address the Sub-Committee on European Relations about current DHS-European Union initiatives. I also want to thank Director-General of Justice and Home Affairs Jonathan Faull from the European Commission who has come a great distance to join me here today. I am very pleased with the progress that DHS and the European Commission are making in addressing many issues of mutual concern related to combating terrorist threats, transportation security and border enforcement.

As you know, the U.S. has an especially close partnership with the European Union, and, since its formation, DHS has been a key player in establishing many transatlantic initiatives and agreements. The challenges of the post 9/11 environment can only be tackled and surmounted with the cooperation and assistance of our European partners and other foreign counterparts.

The challenge before us is to secure the Homeland from another terrorist attack while preserving our most cherished values and maintaining a free, safe and open society. DHS is diligently working to improve its ability to identify terrorists and criminals without impeding legitimate trade and travel. While we are enhancing security by reexamining how we produce and examine documents, bolstering security at our ports of entry, and improving and expanding watchlists, we are committed to protecting and respecting the civil liberties and individual privacy of US citizens, residents, and visitors. Our efforts to combat terrorism threats and protect our borders require the assistance, counsel and partnership of our allies, especially our transatlantic neighbors in Europe.

The recent bombings in Madrid, Spain caution us that terrorism is an international threat that cannot be conquered alone. Moreover, the recent events demonstrate that Al-Qaida-influenced regional extremist networks have increased in visibility and may pose a growing threat to the U.S. and the rest of the world. As such, we must engage in a global effort with our colleagues in the European Union and elsewhere on a daily and even hourly basis to make sure that our lifesaving work is thorough, sound and coordinated.

As part of this effort, we are working well with our partners on improving standards for travel documents, aviation safety, and the exchange of watchlist information. In an effort to scrutinize travelers more effectively and more equitably, we are moving toward individualized review. Appropriate and secure use of biometric identifiers will significantly aid this process. Biometrics will also assist our efforts to authenticate the identity of travelers. By individualizing the process through biometrics, we can be more confident and secure about our admissions and screening decisions. To

get there, we are working closely with our European counterparts in the International Civil Aviation Organization (ICAO) and other fora to discuss how to advance biometric methodologies, both in chip technology and electronic readers. International discussions on these issues are vital, specifically in regard to how we can best address privacy concerns.

In addition, we are building a layered approach for aviation security. DHS recognizes that there is no single solution to prevent airplanes from being used as weapons of mass destruction. The layered approach includes enhancements to visas, appropriate use of airline passenger data, vetting travelers through US-VISIT, boosting airline security utilizing air marshals on international flights of concern, and offering voluntary programs for arming pilots on the passenger and cargo planes for domestic flights. DHS fully recognizes that imposing unnecessary inconveniences will discourage travel to the US and is committed to avoiding unnecessary procedures that would harm the United States' ability to welcome students, tourists, and business travelers. Our investments and efforts within the transatlantic and international context aim to minimize burdens on our citizens' and visitors' livelihoods while we pursue our main mission of protecting their lives.

We are working closely with EU Director General for Justice and Home Affairs, Jonathan Faull, and other officials and agencies of the European Union to ensure that developments and initiatives in aviation security are discussed, coordinated, and explained before they are implemented. Through on-going communication and dialogue with the EU we are seeking to avoid transatlantic surprises and diplomatic differences. As we move further into the 21st Century and adopt biometric technology and other advancements, we will proceed with prudence and deliberation, considering the civil liberties effects of governments' use of these technologies and ensuring that we fortify our privacy protections so that no personal data can be misused or abused.

We are taking such steps every day. Let me briefly touch on some of the ongoing discussions we are having with our European partners that can be viewed as true achievements and positive, practical steps to tackle the security challenges we face together.

Lost and Stolen Passports

Together with our colleagues in the Department of State, who are responsible for the U.S. passport system, and our foreign counterparts, DHS is addressing security challenges posed by lost and stolen passports. We share this effort with our partners in Europe and around the world. Across the globe, international border control authorities continue to seek timely and accurate information concerning the validity of travel documents presented at their borders. In most cases, countries are able to identify the misuse of their own lost or stolen travel documents when presented at their own borders; however, without a system for international sharing of this data, to date it has not been possible to access this data from other countries. Finding the best solution to this security challenge is the topic of discussion in many international fora. In addition, this is an

important discussion that DHS has with most every foreign delegation that it hosts and that it visits.

Additionally, DHS is following efforts made by the ICAO New Technologies Working Group which has undertaken preliminary research into using Interpol's electronic global data base to exchange information on lost and stolen passports, so that a query of country and passport number can be submitted to a central database of lost and stolen passports. The long-term goal is to develop a system in which a yes-no response can be generated in real-time. We support these efforts and see these advancements in the exchange of information as key to securing our borders.

Recently, the Department of State announced a new a program through which the U.S. will provide current information on issued passports that have been reported lost or stolen to the Interpol's lost and stolen document database, which is available to border authorities worldwide. The Department of State has just transferred to Interpol data on 330,000 lost or stolen U.S. passports. Only the passport number, country of issuance and document type will be provided to Interpol. We believe that this action will encourage other governments to join in this international data-sharing initiative.

Container Security Initiative (CSI)

On April 22, 2004, the United States and the European Community signed an agreement to intensify and broaden cooperation on customs matters. The objectives of the agreement include, among other things, the prompt expansion of Customs and Border Protection's (CBP) Container Security Initiative (CSI) to more ports in the European Community.

The Container Security Initiative addresses the threat to border security and global trade posed terrorist misuse of a maritime container. The purpose of CSI is to ensure that all containers that pose a potential risk for terrorism are identified as early as possible in the international trade supply chain and before they are laden on board vessels destined for the United States. CBP is now stationing multidisciplinary teams of U.S. officers from both CBP and U.S. Immigration and Customs Enforcement (ICE) to work together with their host government counterparts. Their mission is to work with local law enforcement officials to develop additional information related to the terrorist threat to cargo destined to the United States.

Through CSI, U.S. officers work with host country customs administrations to establish security criteria for identifying high-risk containers. Those administrations use non-intrusive technology to quickly inspect the high-risk containers before they are shipped to U.S. ports. Additional steps are taken to enhance the physical integrity of inspected containers while en route to the U.S. CSI ports are points of passage for approximately two-thirds of containers shipped to the United States.

The CSI agreement signed last month with the EU sets the stage for enhanced cooperation between the United States and the Europe on CSI and related matters. It will lead to enhancements in our mutual efforts to prevent terrorists from exploiting the

international trading system. The agreement will intensify and broaden cooperation and mutual assistance in customs matters between the European Community and the United States. The objectives of the broadened cooperation called for under the agreement include expanding the Container Security Initiative, establishing minimum standards for risk-management techniques, and improving public - private partnerships to secure and facilitate international trade.

CSI is a fully reciprocal program. Japanese and Canadian officers are currently stationed and working in key U.S. ports to screen containers destined for their respective countries. We expect others to do so in the future.

While the first twenty largest ports (which include many in Europe) were the starting point, CSI is not limiting participation to those locations. Sweden, Malaysia, South Africa, and Sri Lanka have signed on to CSI: ports in the first three countries are already operational. Discussions are currently being held with additional expansion ports in South and Central America, Southeast Asia, and the Middle East.

International organizations like the World Customs Organization has provided a multi-lateral forum for discussion of appropriate security measures and encouraged the further development of CSI-type initiatives throughout their 162-country membership.

Passenger Name Record (PNR) Data

In addition to expanding cooperation on container screening, the U.S. and the European Commission (Commission) have been able to move forward with a negotiated arrangement for screening passengers. During my tenure with Border and Transportation Security (BTS), I have been the lead negotiator for the U.S. with the Commission in our efforts to establish a legal framework to allow CBP, a component of BTS, to access passenger name record (PNR) data from the airlines that carry passengers between Europe and the U.S. In 1995, the European Parliament and Council issued a "Data Protection Directive" which sets forth detailed requirements for the utilization and sharing of personal data. The purpose of our negotiations with the European Commission is to obtain an adequacy finding, under the European privacy directive, which would allow CBP to receive PNR data from those airlines affected by the Directive. Without resolution of these issues with the Commission, airlines would be put in a position where they would be subject to fines from EU member states if they provide PNR data to the U.S.

PNR data is just one of many tools used by CBP to fulfill its mission. PNR data is an essential tool in allowing CBP to accomplish its key goals: (1) PNR data helps us make a determination of whether a passenger may pose a significant risk to the safety and security of the United States and to fellow passengers on a plane; (2) PNR data submitted prior to a flight's arrival enables CBP to facilitate and expedite the entry of the vast majority of visitors to the U.S. by providing CBP with an advance and electronic means to collect information that CBP would otherwise be forced to collect upon arrival; and (3) PNR data is essential to terrorism and criminal investigations by allowing us to link information about known terrorists and serious criminals to co-conspirators and others

involved in their plots, including potential victims. Sometimes these links may be developed before a person's travel but other times these leads only become available days or weeks or months later. In short, PNR enables CBP to fulfill its anti-terrorism and law enforcement missions more effectively and allows for more efficient and timely facilitation of travel for the vast majority of legitimate travelers to and through the United States.

Through these negotiations (which have been going on for more than a year), we are grateful for the cooperation of the European Commission. Last December, the European Commission agreed to adopt an adequacy finding and just this week, the 25 member states accepted the finding in the Article 31 Committee vote. Over the course of our negotiations, Both sides worked together to reach a workable solution that outlines the type of data that may be transferred, the period of time it can be retained, and the purpose for which it may be used. Additionally, the arrangement includes requirements for aggressive and important passenger redress mechanisms including a channel for direct access by European Data Protection Authorities to the Chief Privacy Officer at the Department of Homeland Security on behalf of European citizens.

While implementation is pending a final review by the European Council, we are encouraged by the Commission's efforts, especially the support we have received from European Commissioner of Internal Market, Frits Bolkestein; Commissioner for External Relations, Chris Patten; Commissioner for Justice and Home Affairs, Antonio Vitorino and Director General Faull. While our arrangement and the adequacy finding may face legal challenges, we are confident that they are legally sufficient and will improve the safety of air passengers. When the arrangement is finalized, it will be a historic achievement that will protect both the privacy of travelers and the borders of the United States and the European Union.

Moreover, DHS is also very pleased to learn through the March 25 EU Summit Statement on Combating Terrorism that the EU is itself considering setting up its own PNR system that will further strengthen the ability of the international community to identify the handful of violent criminals and terrorist hiding among the throngs of legitimate travelers.

.

Visa Waiver Program and US-VISIT

I now turn to the issues surrounding the Visa Waiver Program and US-VISIT. As you know, in September 2004, DHS will expand US-VISIT checks to Visa Waiver Program travelers.

The US-VISIT system was initiated on January 5, 2004, and as of late April, the US-VISIT program had processed over 3.5 million travelers without negatively effecting wait times. During that same period, US-VISIT has identified 180 known or suspected criminals and more than 100 immigration violators, including rapists, drug traffickers, credit card and visa fraud criminals, manslaughter suspects, and an armed robber. In most cases, biographic information alone would not have led to the identification of these criminals

Although the US-VISIT Program was initially designed for travelers from non-Visa Waiver countries, its successful deployment demonstrates that it can be effectively expanded to travelers from Visa Waiver Program (VWP) countries who enter the United States at air and sea ports. This expansion will increase security by ensuring that biometric information on VWP travelers is collected even if the deadline for biometric passports is extended.

The biometric passport deadline was established by the Enhanced Border Security Act (EBSA), which requires VWP countries to certify by October 26, 2004, that they have a program to issue biometrically enhanced passports that comply with International Civil Aviation Organization (ICAO) standard. If they cannot make such a certification, they will be unable to continue to participate in the VWP. Additionally, beginning on October 26, 2004, VWP applicants with non-biometric passports issued on or after October 26, 2004, will not be eligible to apply for admission under the VWP. While most VWP countries will be able to certify that they have a program in place, due to technological limitations, they will be unable to actually produce biometric passports by that date. Limiting VWP participation could lead to serious disruptions to travel and tourism because millions of VWP travelers may choose not to travel to the U.S. resulting in billions of lost revenue to the U.S. economy. It may also cause friction with some of our closest allies in war on terror.

The EBSA also requires DHS to deploy passport readers to authenticate these passports. Acknowledging the limits of the current state of technology, Secretary Ridge, on April 21st, testified before the House Committee on the Judiciary that DHS, "…is not currently in a position to acquire and deploy equipment and software to biometrically compare and authenticate these documents. DHS cannot today acquire one reader that will be able to read all chips utilized in the ICAO compliant biometrics passports. However we believe that by the fall of 2006, the technology required to implement successfully a security system based on the ICAO standards will be much more settled and allow DHS to derive benefits envisioned when the original EBSA was enacted." Accordingly, DHS and DOS jointly requested that the October 26, 2004, deadline be extended to November 30, 2006 for the production of ICAO-compliant biometric passports and the deployment of equipment and software to read them.

The VWP governments are deeply concerned about their nationals losing the ability to travel to the United States visa-free and support the Administration's request for an extension. Additionally, the VWP countries understand that in the short-term enrolling VWP applicants in US-VISIT would alleviate some of the security concerns associated with that extension and in the long-term will improve document and border security.

U.S.-EU Dialogue

On April 26, Under Secretary Asa Hutchinson traveled to Brussels to lead a U.S. delegation to the inaugural meeting of the new Policy Dialogue on Border and Transport Security. The EU delegation was led by Director General Faull. The purpose of this new group was to establish a forum where the issues of transport and border security could be

addressed at a policy level. This first semi-annual meeting successfully discussed a wide range of issues and included experts from Homeland Security, Justice, and State on the U.S. side and the European Commission Directorates of Transport, Internal Market, Justice and Home Affairs and External Relations, demonstrating an effort by both sides to bring all concerned parties to the table and avoid compartmentalizing. This on-going formal dialogue is to provide a mechanism to communicate problems or initiatives on the horizon.

Delegates at the inaugural meeting took the opportunity to address many of the issues I have already discussed, including biometrics, the US-VISIT and Visa Waiver Programs, joint initiatives on lost and stolen passports, "flights of concern" and air marshals. With the US-EU Summit approaching in June, parties are already working collaboratively toward making that event a success.

Coordinated efforts and continuous dialogue are certainly the key elements to a successful transatlantic strategy. I am honored to have this opportunity to share the podium with Director General Jonathan Faull, who has been a true ally to the U.S. Specifically, his support and cooperation have been invaluable to DHS as we carry out our daily mission and meet formidable challenges. I am certain that we both agree that the key to staying the course and meeting the great challenges ahead is continuing not only to build and develop technical connections and enhanced methods of appropriately exchanging information but, more importantly, to strengthen relations and communications between leaders on both sides of the Atlantic.