Remarks prepared for

Thomas Marten
Vice President Government and Security Solutions
SITA

At the
European Aviation Club Luncheon

March 13, 2008
Hotel Bristol Stephanie, Brussels

Good afternoon. It's a pleasure to be with you here today in Brussels. Brussels has become a bit of a home away from home for me, for two reasons. First, because the European Commission has become quite active in the area of Border Management and aviation security. That has kept my SITA colleagues and me -- many of us here today -- very busy. Secondly, because one of my brothers recently completed his third tour of duty in Iraq and is now assigned to the American Embassy here. He loves it, and now I have family in Brussels.

I would like to thank the European Aviation Club for extending this invitation today, it's an honor to follow many of the leaders of the Aviation Sector up to this podium, including the CEO's of British Airways, Ettihad, and Easyjet, and officials from the EU Commission and my former colleagues the US State Department.

Let me just say in that regard that one of the advantages of being out of government service is you can say exactly what you think, and that is what I intend to do today.

But first, I have a confession to make: I came to Brussels this morning by train from Paris. In fact, I'll admit it; I'm a big fan of the TGV. I take it regularly between my office in Geneva and my home in Paris. I could have flown, and I do enjoy flying, in fact I fly over 300K miles each year to do my job. But I do choose the train when I can. The main reasons is to avoid the hassle of security at the airport: the inevitable Long lines, the occasional undressing, the sometimes humiliating treatment of passengers, the constantly changing requirements, and the odd mixture of seasoned travelers and novices.

The point is we could do this a lot better. In fact, in many countries around the world we do do it a lot better. There are two sayings about security and borders. The first is that a perfectly secure border is one that no one ever crosses. Obviously that's the

wrong solution for us. The second is that the best security is invisible, both to the traveling public and to potential criminals and terrorists. That is the right solution.

Facilitation and security – those are the twin themes of my discussion today. My message is that you don't have to generate long lines, or make travel unpleasant, or violate individual privacy, in order to make borders more secure. With the right IT solutions, you can do both.

The fact is that when I travel around the world to meet with governments, I find they all want to adopt the same solutions we'll talk about today – APIS, PNR, eVisas, biometrics – but for different reasons. In North America and Europe governments are focused on security and fighting crime. After 9/11 and the Madrid and London bombings, that makes sense. But in the Persian Gulf, in Africa, and in South East and North Asia, governments are looking at the same IT solutions to facilitate travel, to move more people through bigger airports in a way that makes them want to come back.

Let's first take a look at challenges facing the industry, and in particular the aviation industry in Europe.

- **Growth of traffic**: International passenger demand grew over 7% in 2007. European traffic will continue to grow, driven by three factors: the accession of new states to the EU and the extension of Schengen space, the deployment of new Airbus aircraft globally, and the development of new mega-airports in the Middle East and Asia.

  Let's call this the Facilitation challenge facing the industry.

- **Growth of Security concerns (post 9/11)**: In the wake of the 9/11 attacks in the US, and the bombings in Madrid, London, and Bali, governments simply can't ignore the threat of international terrorism. A number of countries – the US, Canada, Australia, Korea – just to name a few, are already placing increasing demands on the aviation industry to provide passenger data or capture biometrics. Providing this data can be an operational nightmare for airlines. The new US proposal, for an interactive APIS system called AQQ, or Advanced Quick Query, poses significant challenges to airlines' IT systems.

  Providing this data can put airlines between a rock and a hard place. For instance, US requirements for PNR data, combined with strict data protection rules in Europe, means airlines which comply with US rules are potentially liable to lawsuits from EU nationals whose sensitive personal data has been exported without consent. The EU Agreements with the US and Canada have addressed many, but not all of the privacy concerns in Europe. But in the coming years

European airlines will face similar demands for data from countries in Asia, the Middle East, Africa, and South America.

Let's call this the Security challenge facing the industry.

- **Other challenges**: Let me just tick off some of the other challenges. First, **M&A**: Two major mergers in Europe are proving that cross border consolidation can deliver solid results: Lufthansa and SWISS, Air France KLM. If merger rumors in the US are correct (e.g. Delta and Northwest), we could see changes there as well. Second, the **cost of oil**: Oil is pushing past US$100 per barrel and accounting for 30% of operating costs of the industry. These costs may be augmented by new **carbon taxes** or other environmental schemes. This in turn will impact the **profitability** of industry: In the five years following the 9/11 attacks in 2001, the industry lost US$40 billion. Airlines finally turned a profit in 2007: US$5.6 billion on revenues of US$490 billion. The challenge will be sustaining and building on that modest level of profitability. Finally, the impact of the ongoing **downturn in the US** will pose challenges on transatlantic routes for which the **US-EU Open Skies agreement**, which goes into effect end of this month, may or may not compensate.

  I'll leave it to other speakers, including Mr. John Byerly of the State Department, who will be standing here in two months, to address these challenges in detail. The bottom line is that the industry has been through a long slump, and is just now getting back on its feet. The last thing it needs is another terrorist attack, or the sort of draconian – and usually misguided -- security measures that drive up costs and drive away customers. It's a question of balance.

Focus on Security, and focus on Europe

First off, let me say for the record that I think Europe has got it right when it comes to border management and security. On the one hand, you have the Commission initiatives, led by Vice President Franco Frattini and Director General Jonathan Faull, pushing hard for adoption of many of the measures used around the world to enhance security. As I've said before, these measures, if done right, are the same measures that support facilitation of passenger traffic. In other words they enhance security in a way that is transparent to the traveler.

Let me give you an example: last year's miSense trial at Heathrow Airport. The trial was intended to test of some of the concepts underlying the UK's eBorders initiative. It also served to verify the IATA vision of "Simplifying Passenger Travel," by automating and streamlining airline business processes and immigration and security checks at the airport. SITA worked on this project with a number of other firms including Accenture, Raytheon, Sagem, Cathay Pacific and Emirates Airlines. It included biometric identity

checks of travelers and watch list checks with interactive APIS. It worked brilliantly. The marketing folks generated reams of metrics from customer interviews. The metric that struck me most was that over 70% of travelers felt the chief benefit was faster journey times. Imagine that, a security solution that actually makes travel more pleasant.

The second thing that Europe has got right is the focus on privacy. I am afraid the American public has missed the plot on this issue. I salute the work of the many members of the European Parliament to make sure that any security initiatives adopted in the EU, or imposed on EU carriers by third countries -- like the US or Canada -- are consistent with democratic values. I do not agree with extremists who seem to think that the only way to preserve democratic values is no security. I think you have to find a balance. I believe Europe is uniquely positioned to find that right balance because of the vibrant debate which goes on here.

Taken as a whole, the recent Commission Proposal on the Use of Passenger Name Record (PNR) data, and the Communication "New Tools for an Integrated Border Management Strategy" represent a coherent approach to enhancing the security and safety of Europe's borders. They build on the so-called Spanish Directive (Council Directive 2004/82/EC), which created a framework for the provision of Advance Passenger Information (APIS) to the competent authorities of Member States.

Certain aspects of the border management system proposed by the Commission are in use in a number of countries worldwide, including the United States. In many cases, such systems were deployed in piecemeal fashion, or are only partially adopted. The Commission's approach is unique in that it will enable Member States to adopt a harmonized approach, guided by a coherent vision. That vision must seek a balance between security and law enforcement objectives on the one hand, and considerations of cost, data privacy, and travel facilitation on the other.

There's a lot to like in what I'll call the EU Border Management vision. Like an American bride, it has something old, something new, something borrowed, and something blue.

Something Old: the Spanish Directive

The Spanish Directive was adopted in April and entered into force fairly quietly in November 2004. It established a legal basis for Member State to require Advance Passenger Information (APIS) data from the airlines. It was called the Spanish Directive because it was pushed through the Council by Spain, in the wake of the Madrid bombings of March 2004. The Spanish Directive has attracted little attention, mainly because there is no privacy controversy. APIS data is little more than the data in your passport – first name, last name, passport number, date of birth, etc. – which is usually

provided when you cross a border anyway. I know of no privacy advocates anywhere who have raised concerns about APIS data.

At the simplest level, APIS data allows a government to check passengers against various lists of "bad guys" or undesirables. These could include terrorist or criminal watch lists, lists of lost and stolen passports, eVisas lists, or lists of immigration law violators. This

can help speed up processing upon arrival; the immigration or border police already know if someone requiring special attention is on board. In fact the Mexican government uses an APIS system at Cancun Airport to move entire aircrafts full of passengers through customs and immigration quickly: if everyone checks out on a flight landing at rush hour when the immigration queues at Cancun are longest, they'll pull all the passengers out of the line and send them directly to their hotels to enjoy their vacation.

The problem with legacy APIS systems like the one described in the Spanish Directive is that if you do identify a bad guy on a flight after takeoff, it's a little late. You may already have a serious problem with a tank full of kerosene fuel coming your way. Hence the push in the US and UK to move to an interactive APIS system, like Australia, but that's not yet on the European agenda.

Something New: Draft PNR Directive

On 6 November of last year the Commission adopted a proposal on the use of Passenger Name Record (PNR) data for law enforcement purposes. The proposal establishes a legal basis for the acquisition and processing of PNR data by EU Member states in order to fight terrorism. Unlike the Spanish Directive, this one is controversial. A Passenger Name Record (PNR) is a record in the database of a Computer Reservation System (CRS) that contains the travel record for a passenger, or a group of passengers traveling together. PNR's contain a lot of information useful to airlines, travel agents, and incidentally, to law enforcement. This includes ticket and itinerary data, and payment data. From a law enforcement perspective PNR's are doubly useful: they can help governments identify high risk travelers who merit special attention upon arrival at the border (but who may not be on a watch list). This is called risk assessment. PNR's can also be extremely useful for after the fact crime investigations and forensics.

The US Government has been using PNR data for border security for over a decade. Canada adopted a PNR solution shortly after the 9/11 attacks. The US programs attracted a lot of attention from privacy advocates in Europe. In 2006 privacy advocates in the EU Parliament successfully challenged the US-EU Agreement PNR Agreement before the European Court of Justice. Although a new Agreement was signed in 2007,

there is still considerable concern about how "sensitive" personal data is handled in the US.

In contrast, the EU-Canada PNR Agreement of 2006 has gotten hardly any notice at all. That is unfortunate, because it is exactly the sort of Agreement that could serve as a template for a European PNR Framework. It demonstrates that it is possible to reconcile the apparently conflicting national priorities of security and privacy. The EU-Canada Agreement involves the use of a PNR Push/Filter to filter out sensitive data fields identified by the EU Commission in the UK, and transmitting ("pushing") only the filtered data to the Canadian Government. This system is popular with the airlines, with privacy advocates, in the EU Parliament, as well as with the relevant governments. Airlines like it because it protects them from potential lawsuits from EU citizens for violating their privacy. Privacy advocates like it because no sensitive personal data is ever exported from Europe. The Canadian government likes it because they get the data they really need to secure their borders, without the headache. The system was designed by SITA, and it is the baseline we use in discussions with Governments and airlines around the world to ensure compliance with EU privacy rules.

This is why I think it is critical that the EU develop a coherent policy framework for PNR. Harmonization is part of the story -- several Member States are already moving ahead with PNR programs. More importantly, the EU will always be at a disadvantage in international negotiations related to PNR as long as it negotiates from the other side's text. A European framework would serve well in future negotiations with third countries which are now adopting PNR systems. Most importantly, a European framework that strikes the proper balance between security and privacy would serve as a model for security programs around the world, and that, in my view, would be a very good thing.

Something borrowed: EU Package of Border Management Initiatives

The last piece of the EU border management package is the set of measures announced one month ago by M. Frattini, including an Electronic Visa system and a biometric entry/exit control system. Both initiatives are borrowed from programs announced or adopted in the United States. Both have very long fuses, with adoption unlikely for several years.

Both initiatives were originally announced in a "tit for tat" fashion by the Commission, in response to new requirements imposed by the US on EU citizens. In the world of diplomacy we call this reciprocity. More importantly, both programs are included in the IATA SPT vision. That means that if properly implemented, these measures would generate significant progress in terms of facilitating passenger movements, reducing costs for the industry, and enhancing security.

Taken together, these four programs, which I have referred to as the EU Border Management Vision -- APIS, PNR, eVisas, and biometrics – point forward to the future of border management. That future lies in the convergence of biometrics and passenger data exchange systems. In a few years we will all have biometric passports, and as we move through airports and across borders we will be able to move more quickly, at lower cost, thanks to these technologies. The key will be to protect our privacy as we move forward.

Well I promised you something old, something new, something borrowed and something blue. I think we've covered the first three, but as for the last one, all I can do is say sorry, this is winter in Belgium, and the skies are grey, not blue. I mentioned security earlier, but lousy weather also makes for a good day for trains. My trip in from Paris this morning was a charming ride, I was able to get up and walk around, and the train took me from city center to city center. But just ask me again next Fall when the French rail unions go on strike, and I'll probably tell you I'd rather take the plane. And if we do manage to get this security and facilitation balance right, we'll all enjoy flying again, all the time. Our industry will continue to grow, providing secure, safe, and genuinely pleasant travel services to bring people in Europe closer to their families, their friends, their business associates, in the Americas, in Asia/Pac, in Africa, and in the Middle East.

With that, let me close, and let me say thank you for your kind attention. Enjoy the rest of your meal: I'd be happy to take any questions, now or after lunch. Thank you.

SITA
March 2008

For further information, please contact:

Thomas Marten
VP Government & Security Solutions
SITA - 26 Chemin de Joinville
1216 Cointrin, GE - SWITZERLAND

Tel: +41 22 747 6828
PA: +41 22 747 6211
Mobile: +41 79 320 8921
e-mail: thomas.marten@sita.aero

Matthew Finn
Director, Government & Security
SITA - 26 Chemin de Joinville
1216 Cointrin, GE - SWITZERLAND

Mobile: +41 79 615 5212 (mobile)
Mobile: +44 7834 140 268 (mobile)
Tel: +41 22 747 6689 (office)
e-mail: matthew.finn@sita.aero