I am pleased to participate in this very important gathering and to discuss biometric based identity management in the context of immigration and border security. This is an exciting time to be part of the biometrics industry – both because we have the opportunity to offer solutions to critical national challenges, and because we are at the forefront of a fast growing business with strong investment potential.

IBG projects that the total biometrics market will generate more than $7 billion in sales by 2012, growing at a rate of approximately 20% annually. The Civil ID segment, where immigration and border control are included, is estimated to grow faster than the overall biometrics market--as much as 30% annually over the next three years--and to reach $3 billion in annual revenues by 2012. Most of this growth is being driven by the public sector-- and that is why those of us in the private sector value venues like this, where we are able to connect with the public sector to better understand your challenges and the broader public policies to which we must respond. This process helps us create real value for our investors and for the public.

This “intersection” of public policy and private technology development is shaping our marketplace in ways that have a significant impact on the industry’s bottom line, and on the government’s ability to secure the commonweal. The urgent need to move forward with “person-centric” identity management systems to achieve a host of public policy objectives--from the most critical national security issues to verifying employment eligibility to the prevention of fraud in domestic social programs---underscores the importance of government-industry collaboration to define in real time both the challenges we face and the solutions to them.

Today, moving people and goods across borders securely and efficiently has never been more important to global stability and economic prosperity. At the same time, however, threats to international security have never been more elusive or clandestine, or, unfortunately, real. Hence the demand for efficient and secure identity management systems has never been higher.
I have been asked to focus my remarks today on immigration and border control and I am pleased to do so because, in its broadest definition, the concept of borders envelopes a very large part of the national security agenda. Also, border control—in its largest context—is a significant part of the roadmap for creating value in the biometric-enabled identity management business. First, let me explain how I envision the border and what I mean by border control.

Border control is often described in the same breath as immigration control. However, border control has many dimensions, only one of which is the regulation and tracking of migratory flows. Border control goes well beyond the Border Patrol intercepting illegal aliens or an immigration official deciding who can enter the United States either temporarily or permanently. Our border control system begins far beyond our physical borders—for example, Department of State Consular Officers abroad decide whether to grant visas to persons seeking admission to the United States. Although not undertaken at the physical border, this is clearly a border control activity.

Border control also encompasses regulating the flow of inanimate objects such as cargo destined for the United States. A system designed to intercept and prevent the importation of objects harmful to the United States is as much a border control function as the prevention of terrorists from entering the country.

Our border control system manifests itself again and most obviously at our actual geographic borders, both at designated ports of entry and the areas between them. This is where people and goods seek real time permission to physically enter, or where entry is attempted illegally.

Our border control system also manifests itself in the interior of the country where people who gained entry illegally, or who have overstayed their time of admission, are subject to detection and deportation. Likewise, the interception of harmful or illegal goods that have evaded detection upon entry is another element of a seamless border control system.

The border control system also functions in the interior of the country in other ways such as providing opportunities for people to adjust their status and to gain authorization to legally work in the United States. For example, the I-9 program, which is designed to verify a person’s eligibility to work in the United States, is very much a border control function. All of these functions are part of a system to defend our nation’s right to control its borders and to know who and what is inside the country and what they are doing.

As you can see, our borders are not a particular place, but a continuum along which we must maintain unbroken control. This continuum represents an important piece of the value chain in the identity management business and presents significant opportunity for those of us who believe in its investment potential.
Developing solutions that capture value across the whole spectrum is a winning business model.

Today, technology developments are allowing us to rethink the fundamentals of how we manage our borders and deal with migratory flows. During this decade, the United States and many other nations around the world have built immigration policy and cargo control frameworks in which advance information, data-mining and analysis, pre-screening tools, and real-time identification technologies are used cooperatively to identify threats and assess risks as early as possible-- and to establish protocols for appropriate levels of response.

Within this evolving architecture for managing our borders, biometric-based identity management is at the core of a risk-based, person-centric approach--from direct border control initiatives such as EU biometric visas and the US-VISIT Program, to managing access to port facilities, securing critical infrastructure, and improving emergency response capabilities. It doesn't take much imagination to understand the significant business and investment potential that is presented by the growing need for systems to manage these programs now and in the future.

As I mentioned earlier, our borders begin far beyond our territorial boundaries. We cannot truly protect our borders--nor can any other sovereign entity protect its--unless we face this challenge as a global community. Governments globally must work together if we are to build a bulwark against the mobility of terrorists and others who do not respect the sovereign right of nations to protect their borders in the broadest sense. I can tell you that our business strategy at Cross Match is based on a vision of internationally interoperable systems that will facilitate effective border control.

But as an industry we are still in the early stages of implementing comprehensive biometric identity management solutions, particularly in the area of systems that provide reliable and real time identification in a host of different environments—or in the common parlance of our business—providing multimodal capabilities. Trends in development include multi-biometric fusion, enhanced mobile and wireless capabilities, combining biometrics with behavioral pattern recognition, and “contactless” solutions such as reliable real time facial recognition, mobile iris capture, and iris-on-the-move. If you have an opportunity to visit the Cross Match and other booths in the exposition hall, you will see some good examples of this type of forward-looking technology and how it can be used to provide security for people and property in a wide array of environments.

As we all know, demand is fueling rapid technology innovation in the biometrics arena. Three specific factors have driven growth over the past few years. First, there is the influence of "Moore’s Law" of faster, cheaper processing power. We are seeing this everywhere, especially in the embedded computing and smartcard areas. Second, advances in digital imaging continue at a fast pace, driving the development of cheaper, faster, and more accurate biometric devices and systems. And, third, advances in communication and encryption technologies are
enabling instant, affordable, and secure access to threat assessment and other
information by personnel and systems that require such access to operate effectively.

These trends will continue to have a significant impact on our business. In
some applications, biometric identification will morph from a recognized activity to a
remote, inconspicuous function. Multiple biometric modalities will often be fused so
that biometrics alone will be enough to identify an individual. It seems inevitable that
biometrics will become an everyday part of life – an innocuous function designed to
assure that you are a trusted person with access to all the actions and freedoms to
which you are entitled, thereby sometimes—but not always—obviating the need for
credentials, passwords and the exposition of biographic data.

This technological progress and the added security notwithstanding, identity
management programs face reasonable criticism and other significant challenges.
Consider the airport community, where privacy and cost issues are driving concerns
over the viability of implementing a biometric exit program. In addition, harmonization
of the many expanding border and immigration management programs has proved
challenging—privacy, costs, and overlapping programs are just the tip of the iceberg,
as the landscape is rife with other obstacles such as lack of connectivity among
legacy systems, disparate program initiatives, and physical and technological
challenges with implementation.

Additionally, users rightfully insist that they be able to trust and verify that a
government or commercial system really has protected and deleted private data in
accordance with articulated policies. As international systems develop, they must not
only be interoperable through the application of standards, but they must be
transparent at the policy and process levels as well, so that biometric data can be
trusted, and the entire biometric process can be securely audited. These are the
challenges that represent business and investment opportunity for those of us who
are focused on providing comprehensive identity management solutions.

Worldwide, nations are struggling to formulate comprehensive immigration and
border control policies that strike the right balance of openness and security, while
promoting prosperity. Many European countries have been working to address this
challenge for years—with few arriving at satisfactory solutions. Aging populations
and the social welfare and demographic requirements of economic growth suggest
that legal immigration will necessarily be encouraged in Western European countries,
as well as in the United States. But increased immigration does not come without
short-term consequences such as the potential impact on domestic social services
and the increased need for information, transparency, and security in the admission
process.

Even countries with reasonably well-established immigration policies are
struggling to implement visa, asylum, permanent residency, and naturalization
programs that achieve balance among economic concerns, the values of their
societies, and growing security requirements. With migratory flows on the rise,
nations worldwide are finding it necessary to adopt policies and programs that incorporate rapid and reliable biometric-based solutions for border and immigration management.

The United States is certainly not without its own considerable challenges in implementing rational and enforceable immigration policies. Comprehensive immigration reform legislation that was recently defeated in the Congress, although highly controversial with respect to certain issues, was designed to begin regaining control over our borders in the broadest sense. If what is past is indeed prologue, it is only a matter of time until immigration reform legislation will be resurrected and enacted.

The success of immigration reform, whenever it occurs, rests in significant part on the implementation of systems that improve our ability to definitively establish the right to enter and to verify the identity of those who enter and exit this country.

Although comprehensive immigration reform has stalled, the challenges remain and must still be managed. The demand for guest workers within the U.S. continues to be very high, but the supply line is being stressed with beefed-up enforcement initiatives to identify illegal workers. These initiatives have negative economic consequence for some of our core industries and, needless to say, there is an urgent need to have an effective system to verify the employment eligibility of foreigners who often fill positions in these industries.

Several valuable pieces of the defeated Comprehensive Immigration Reform Act are still on the table, such as those in the arena of workplace enforcement. One example is a bill proposed by Senator Jon Kyl that includes an expansion of DHS’s Basic Pilot Electronic Employment Verification System, now known as E-Verify. Senator Kyl’s bill, the “Immigration Enforcement and Border Security Act of 2007,” would create a “Voluntary Advanced Verification Program to Combat Identity Theft.” If enacted, employers could voluntarily provide fingerprint data of new hires to DHS for identity verification. By doing so, organizations would benefit from a centralized official source for employment eligibility verification, while reducing vulnerability to fraudulent employee documentation.

Biometric technology plays an enormously important role in initiatives such as these. Traditionally, employers have relied on social security numbers to verify the identities of employees. Immigration issues, among others, arise because these Social Security numbers are relatively easy to steal. This form of identity theft, which is commonplace within the non-biometric Basic Pilot program (the Swift case demonstrating the point), clearly illustrates the need for biometric-based solutions.

Earlier this year, Doris Meissner, my predecessor as INS commissioner, and I published a New York Times op-ed piece on this very topic. We noted that a fatal flaw in the Basic Pilot program was that it relied on the authenticity of social security numbers, while being unable to establish that the person presenting the number is in
fact the individual to whom it rightfully belongs. A social security number – or in fact any credential – simply cannot provide the same level of certainty and, hence, security, as a biometric indicator.

Beyond immigration reform, the “Improving America’s Security Act of 2007” recently signed by President Bush—and better known as the 9/11 bill—contains important provisions that will set the stage for even more secure borders. For example, by mandating a biometric exit process as part of the Visa Waiver Program, the Act allows us to complete the circle in making “person-centric” risk assessments rather than relying on outmoded nationality-based risk assumptions. Other provisions in this law, including requirements to screen airport employees, further support risk-based approaches.

There are many facets to successfully incorporating biometric technology into border and immigration management programs. I want to stress three overarching points that I believe are critical to this success and to the long-term growth prospects for our industry.

First, the process of international standards development must continue and move quickly. As an industry, we must embrace global interoperability and move to a stage of development where biometric solutions become truly ubiquitous. They must not only work in tandem, but also within existing security installations. Without an internationally accepted standards-based development process, government bodies and private industries are at risk of making bad investment decisions for less than optimal program outcomes.

The ongoing work of our standards bodies is very important. Under the leadership of Fernando Podio and his colleagues, NIST has developed a comprehensive set of standards that range from application interfaces, interoperable data interchange formats for all types of biometrics, application profiles, and testing methodologies. These standards provide the foundation upon which an international information sharing enterprise can be developed, and that is crucial for the creation of systems that will improve our global security while also reducing identity theft and maintaining respect for the privacy of the users of the system.

The second point involves the importance of building scalable and adaptable systems that can improve and change alongside technology and circumstances. As we develop systems to address public policy challenges, we must ensure that redundancy, privacy, and flexibility are at the forefront. Organizations invest a vast amount of time, effort and financial assets in deploying broad-scale biometric installations and they are looking for those investments to provide a healthy return. Costly programs such as US-VISIT must be designed to be reliable, scalable, and adaptable to leverage emerging technologies without requiring a replacement or fundamental overhaul of the system. That is our challenge, and opportunity, as an industry.
The third, and perhaps the most important point that I’d like to make, involves the critical element of international cooperation in building an identity management framework that is interoperable. Our friends in Australia, for instance, have already implemented an Electronic Travel Authorization system for online visa registration; and through the Smartgate program, they are using facial recognition technology to verify travelers’ identities in conjunction with existing ePassport scans. The U.K. is rolling out its e-Borders program, which will read and authenticate biometric-enabled travel documents on arrival. Additionally, the U.K. will be able to perform biographical, biometric and physical exit checks as part of its registered traveler program for low-risk travelers.

Here at home, we have begun to adopt some of these and a number of other good ideas. For example, the Visa Waiver Program legislation included in the 9/11 Act introduced an electronic travel authorization system. To make the most of these initiatives, we must ensure that they adhere to international technology standards. Interoperability will make biometric solutions and services more attractive and economically feasible for customers worldwide, in both the public and private sectors, and will contribute to international security, stability and prosperity.

Conclusion

In conclusion, I want to reiterate that borders are processes, not places, and borders represent the very essence of national sovereignty and security. As our borders become more “virtual” and the physical lines of demarcation are recognized as being less relevant, internationally interoperable, biometric-based identity management systems become even more important. Moving forward, industry must develop innovative approaches that achieve public policy objectives faster, cheaper and more effectively. This extends across the whole spectrum of activities, from research and development to standards development to program implementation. Better solutions will ensure that our market will continue to grow rapidly and we-- and all of our investors-- stand to gain from this.

In the final analysis, our success is contingent upon governments, system integrators, and technology providers cooperating to meet these challenges. Failure is not an option. The stakes are just too high for all of us who value freedom, security and opportunity.

Thank You