5,500 miles of shared border.

Diverse environments, waterways, terrain, and weather.

Dozens of agencies and programs responsible for public safety and law enforcement.

Two nations, working together to secure the border, facilitate trade, and promote safe travel.

The border between the United States and Canada is as unique as the governments responsible for protecting it. By enhancing collaboration and information sharing on both sides of the border, law enforcement agencies can work together to achieve a safe, secure supply chain for citizens and industry.
“With emerging mission-support technology and new ways to collect and share information, today there are more opportunities than ever for the U.S. and Canada to collaborate at the border. The 2012 U.S./Canada Border Security Summit provided a lively forum for debate among current and future leaders in border security across a range of organizations. This Post Summit Report is intended to capture that discussion, and encourage further dialogue on how both countries can continue to work together to adapt and respond to ever-evolving threats, protect the border, and facilitate international trade and travel.”

— Bob Jacksta, Deloitte Luminary and Former CBP Executive

Bob retired from Customs and Border Protection (CBP) in July 2010 after a thirty-four year career in federal law enforcement. During his career he demonstrated a deep knowledge of customs and immigration issues and a keen understanding of how technologies can be applied to border security. Bob has worked on major border security initiatives with various levels of the U.S. government and international organizations.

As Deputy Assistant Commissioner for the Office of Field Operations, Bob managed border security and anti-terrorism efforts, international trade compliance, anti-smuggling, passenger operations, and oversight of the policies, programs and operations of 20 major field offices, 326 ports of entry, and over 28,000 employees.

During his tenure at CBP, Bob previously served as Acting Assistant Commissioner, Office of Public Affairs, and in a number of other CBP Senior Executive positions with responsibility for national policies and programs in support of radiation detection and non-intrusive technology, supply chain security through Customs-Trade Partnership Against Terrorism, international cargo security through the Container Security Initiative, National Passenger and Cargo Targeting Centers, and advanced passenger and trade information systems.

Bob received a Bachelor of Science Degree from Buffalo State College in New York in 1976. He lives in Virginia with his wife and two children.
Contents

Introduction ............................................................................................................................................. 2

Creation of force-multipliers: increased information and intelligence sharing capabilities ............... 3
  Integrated approaches drive innovation and efficiency ........................................................................... 3
  Challenges to achieving a common vision ............................................................................................... 4
  The path forward – taking joint approaches to the next level ................................................................. 5

Biometrics and identity management: building partnerships and expanding technology to share traveler data ............................................................................................................................................. 7
  Growth in biometric partnerships ........................................................................................................... 7
  Challenges to collecting and sharing biometric data ............................................................................... 7
  The path forward — expanding and scaling biometric capabilities .......................................................... 9

Tools for border security: applying current and future technologies in an effective and efficient manner ............................................................................................................................................. 12
  Enhancing security through advanced technology ............................................................................... 14
  Challenges to implementing next generation technology ....................................................................... 14
  The path forward — shared, risk-based technology to build economies and enhance security .......... 15

Presenters ................................................................................................................................................ 16
Introduction

With over $1 billion in trade crossing through the border each day, it is vital to both economies to manage the flow of goods and persons in an effective and efficient manner without compromising the security of either country.

The U.S. and Canada have been long time partners in border security and management; however, the last several years have seen an increased level of interoperability and shared intelligence efforts. In December 2011 the U.S. and Canada agreed to the **Beyond the Border Declaration and Action Plan**, demonstrating a formal commitment to establishing a new perimeter approach to security and trade. The U.S./Canada Border Security Summit, held on April 3-4, 2012 in Dearborn, Michigan, focused on how the **Beyond the Border** vision of a multi-layered, intelligence-driven approach can be operationalized and driven forward by the agencies and programs responsible for protecting the borders. The Summit brought together thought leaders and key policy-makers across U.S. and Canadian local, state, provincial and federal law enforcement for actionable discussion and debate on several of the key focus areas of the Action Plan.

The topics addressed included:

- **Creation of force multipliers** – understanding how bilateral collaboration and whole-of-government approaches can exponentially increase national security information sharing and intelligence capabilities
- **The next generation of identity management** – developing unified standards for how fingerprints, facial recognition, and other forms of biometrics can be collected and shared to drive the facilitation of travel between countries and the identification of high risk individuals
- **Emerging tools for border security** – building towards the interoperability of technology solutions, systems, and data to create new avenues for information sharing and establish a common operating picture

Covering an expanse almost three times the size of the border with Mexico, with a vast degree of difference in topography, the land and maritime passages shared by the United States (U.S.) and Canada have a specific set of challenges when it comes to securing and managing the border.

Organizations represented at the Summit

**United States**
- Department of Homeland Security (DHS)
- Customs and Border Protection (CBP)
- Immigration and Customs Enforcement (ICE)
- U.S. Coast Guard (USCG)
- U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT)
- Federal Bureau of Investigation (FBI)
- Michigan State Police Emergency Management and Homeland Security Division
- U.S. House of Representatives, Committee on Homeland Security

**Canada**
- Canada Border Services Agency (CBSA)
- Royal Canadian Mounted Police (RCMP)
- Citizenship and Immigration Canada (CIC)
- Canadian Coast Guard (CCG)
- Defence Research and Development Canada (DRDC)

**Other organizations**
- Border Trade Alliance (BTA)
- Canadian/American Border Trade Alliance (Can/Am BTA)

This Post Summit Report highlights the key themes discussed by leaders in the border security mission, including a view of the collaborative work already underway to enhance individual and shared border security efforts, an analysis of the challenges faced by both countries in order to implement the **Beyond the Border** strategy, and a look forward to the future of a risk-based, intelligence-driven joint vision for supply chain security at the U.S./Canada border.
Creation of force-multipliers: increased information and intelligence sharing capabilities

Integrated approaches drive innovation and efficiency

Increased opportunities to develop bilateral partnerships and share information in innovative ways, paired with changing budgetary environments, have led to a dramatic shift in approach to U.S./Canadian border security in recent years. These changes center on a new emphasis on using force multipliers to drive efficiencies – leveraging joint approaches and the leading practices of many different participating agencies to dramatically increase security on both sides of the border. Traditional strategies, including a U.S. focus to “gain, maintain, and expand” control of the border, were unilateral in nature and relied on heavy funding, procurement, and acquisition. This approach is highly resource-intensive and cost-prohibitive to maintain in the current fiscal environment. As the U.S. and Canadian governments move towards increasingly constrained budget conditions, both countries have a renewed focus on identifying synergies and other ways to utilize resources more efficiently.

The response from U.S. and Canadian border agencies has evolved into a new, joint strategy, built on a “wide border” concept with a foundation of intelligence, integration, and rapid response. The Beyond the Border Action Plan calls for the U.S. and Canada to build a shared understanding of the threat environment through joint, integrated risk assessments to prioritize emerging vulnerabilities and enhance individual and shared border security efforts. This approach requires government organizations to be adaptable, using resources where they are needed, when they are needed, regardless of country – both at the physical border and at other critical transit nodes and checkpoints.

In order to accomplish the objectives laid out by Beyond the Border, the U.S. and Canada have focused on increasing collaboration in an unprecedented way. From shared radio frequencies and advanced technology to the exchange of classified intelligence, cross-border partnerships between agencies – including the Royal Canadian Mounted Police (RCMP), Canada Border Services Agency (CBSA), Citizenship and Immigration Canada...
Canada-US Shiprider

Officially known as Integrated Cross-border Maritime Law Enforcement Operations (ICMLEO), Canada-U.S. Shiprider involves vessels jointly crewed by specially trained and designated members of the RCMP, CCG, and USCG who are authorized to enforce the law on both sides of the international boundary line. Working together, armed Canadian and U.S. law enforcement officers are able to transit back and forth across the border to help secure it from threats to national security, as well as prevent cross-border smuggling and trafficking. Canada-U.S. Shiprider vessels operating in Canadian and U.S. waters are subject to respective local laws, policies and procedures and operations are undertaken under the direction and control of host country officers.

- **September 2005**: First Shiprider proof-of-concept initiated in Detroit-Windsor area
- **August 2007**: Simultaneous pilot projects conducted at Ontario-New York and British Columbia-Washington borders
- **May 2009**: Framework agreement signed by former Public Safety Minister Peter Van Loan and Janet Napolitano, U.S. Secretary of Homeland Security
- **2010**: Shiprider operations used to support Olympic Games in Vancouver and G8/G20 Summits in Toronto
- **2012**: Implementing legislation which is required in order to incorporate the agreement into national law and make the program permanent is expected to be passed by Canada’s Parliament.
Challenges to achieving a common vision

While U.S. and Canadian counterparts have recently increased the extent of bilateral programs aimed at information sharing and joint operations, the respective agencies face a set of core challenges that must be overcome to fully realize potential force multipliers that can be created through binational collaboration. Both countries are confronted with the difficult task of overseeing multiple agencies that each play a critical role in national security, and each of those government agencies have their own resource, training, and performance management requirements.

Although further integration between the U.S. and Canada could allow the two countries to operate in a more efficient and effective way, the path forward will require the navigation of their own complex layers of oversight, jurisdiction, authority, as well as the following common challenges:

- **Limited resources** – As the number of programs and initiatives aimed at information sharing has increased, so has the required commitment of resources from participating agencies. U.S. and Canadian border agencies have both noted the difficulty of gathering the necessary resources to have proper representation in bilateral programs.

- **Duplicative efforts** – U.S. and Canadian officials noted concerns with overlapping IBET and BEST missions which can lead to duplicative efforts. Demonstrating this issue, BEST increased its reach to include conducting investigations between the ports of entry, which overlaps with IBET’s scope. In order for these efforts to scale effectively, both countries will need to take a broad approach to managing a portfolio of programs, clarify missions and roles for each, seek opportunities to leverage prior achievements and lessons learned, share training and infrastructure, and focus on the greater priority initiatives.

- **Cultural and legal issues** – Harmonized security procedures are an area of focus not just at the U.S./Canada border but across the globe, and these efforts require a significant degree of international collaboration to be effective. Establishing a unified face at the border requires a breakdown of cultural and legal barriers, ranging from public outreach to passing new legislation. The need to address sovereignty and privacy concerns is central to moving from conceptual agreements and pilot projects to achieving truly operational binational law enforcement programs with shared, cross-designated resources.

The path forward – taking joint approaches to the next level

The Beyond the Border Action Plan provides a roadmap for U.S. and Canadian border security and identifies priorities for achieving the vision, including addressing threats early; trade facilitation, economic growth, and jobs; cross-border law enforcement; and critical infrastructure and cyber security. The agreement highlights several factors that will determine the path forward, and each is highly reliant on the ability to create and leverage force multipliers that will amplify and extend existing capabilities.

The first force multiplier is the development of a common approach to threat assessment, which could amplify the effectiveness of individual approaches to assessing risk. In many regions, U.S. and Canadian border patrol and law enforcement agencies are already working together to identify and prioritize threats in an integrated way, but a common framework is needed in order to scale and expand these efforts. Isolated arrangements have been moderately successful, but are highly informal and generally associated with a specific tactical issue or local operation. Significant progress can be made to expand and formalize these arrangements and better leverage leading practices across the U.S./Canada border. In particular, establishing common assessment criteria and mutual guidelines for identifying, segmenting, and addressing risk is necessary in order for agencies to reach agreement on the high priority risk areas and drive risk-based resource allocation.

Joint risk assessments can only be effective if they are supported by ample information sharing between agencies and governments, particularly as it relates to travelers’ biographic information and risk profiles. Achieving the Action Plan’s stated goal to implement automated biographic information sharing by 2013 and to implement a biometric information sharing capability by 2014 will require significant legal and regulatory action on behalf of the U.S. Congress and Canadian Parliament. Furthermore, the U.S. and Canada must establish clear standards for data exchange and system interoperability in order to coordinate entry and exit systems, which will complement
biographic/biometric systems and facilitate further integration of border-crossing screening and enforcement. If successful, these information sharing technologies will reduce identity fraud, improve screening decisions, and support other enforcement and administrative actions.

In addition to the framework outlined in Beyond the Border, there are additional improvements that U.S. and Canadian law enforcement agencies can pursue in an effort to further support enhanced border security:

- **Expand binational interagency forums and joint operations** – U.S. and Canadian agencies should consider expanding successful interagency forums and joint operations based on shared experience, efficiency, and effectiveness. At the same time, these agencies should re-evaluate programs on an ongoing basis to identify opportunities for alignment and further reduce redundancy created by siloed approaches.

- **Expand risk-based resource allocation on the U.S./Canada border** – Because of the number of agencies that operate along the U.S./Canada border, both governments should support risk-based resource allocation decisions. By combining a holistic view of resources with a full, bilateral risk assessment, DHS, CBSA, and other agencies may be able to more efficiently allocate resources through the creation of policy and guidance designed to integrate resources and deploy them to address identified vulnerabilities.

- **Improve training for border patrol agents** – Currently, CBP operates the Northern Border Intern Program (NBI), which consists of 14 to 15 months of extensive training at the Border Patrol Academy and hands-on experience along the southwest U.S./Mexico border, where agents learn the requisite safety skills, on-the-job knowledge, and experience for U.S./Canada border operations. DHS and CBP should consider expanding this program to include a greater number of northern border patrol and law enforcement agents, including agents from CBSA. Providing this type of training on a cross-agency and cross-country basis can increase the number of resources deployed on the northern border, and create a network of professionals that are able to support collaborative efforts.

One possible way to accelerate the achievement of these objectives is through public-private partnerships. These groups bring together public entities with corporations and non-governmental organizations, and serve as forums for industry to gain access to key governmental decision makers and for governmental organizations to hear directly from stakeholders. Topics may include the international supply chain, trade policies, transportation, infrastructure, tariffs, wait times, and regulations. Public-private partnerships provide an opportunity for open dialogue between government and industry to help improve trade facilitation, make investment decisions, understand the operational environment, and impact governance structures. Increasingly, academic centers of excellence serve as clearinghouses to support public-private partnerships.

By maintaining a clear focus on the Beyond the Border strategy, placing an emphasis on building and scaling successes achieved to date, and leveraging the benefits of public-private partnerships, the U.S. and Canada will be able to make significant progress toward reaching their shared mission of maintaining a safe and secure border and providing integrated, collaborative responses to border issues.
Biometrics and identity management: building partnerships and expanding technology to share traveler data

**Growth in biometric partnerships**
Biometrics is a reliable and universally recognized way in which to manage identities and a critical component to realizing the Beyond the Border Action Plan. 138 countries use some form of biometrics, primarily digital face images, and 61 of those countries use this information for visa decision-making purposes. Many aspects of biometric identification are successful at the U.S./Canada border. A strong partnership currently exists between the U.S. and Canada to share biometric information and further develop the uses of this information. Canada’s CIC is working closely with U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT), part of the National Protection and Programs Directorate under DHS, to design the technology strategy for temporary resident biometrics, a key component to an overall biometric identification plan. The contract to develop this technology was awarded and should be rolled out by 2013. This project specifically focuses on ten-print fingerprints and photographic collection and does not employ iris scans. In addition, the photos will only be subjected to a visual match, rather than automated facial recognition. Initial concerns that collecting this biometric information would cause long lines at airports and impact tourism have been significantly assuaged in recent years, and both citizens and visitors have begun to embrace the approach. As technology continues to develop, both CIC and US-VISIT can expand their efforts to capture additional information and further build biometric databases.

Partnerships between CIC and other Canadian domestic agencies such as CBSA and RCMP are another example of collaboration that currently exists to access, utilize, and share biometric data. For example, when an applicant provides biometric data, RCMP checks the fingerprints. CIC uses the results of the check to make a determination on the applicant’s visa. CBSA then uses the visa photos provided by the applicant to compare and confirm the individual’s identity upon arrival. This cooperation, driven by the use of biometric data, helps to improve the decision making process when evaluating applicants and promotes further sharing of information between agencies. These types of strong partnerships can help to enhance national security by establishing more secure screening tools and methodologies to assess persons entering the country, while also promoting improved flow of people and trade.

In addition to strong partnerships on the U.S./Canada border, there are several examples of effective operational and pilot programs that demonstrate the potential for further expanding the use of biometrics:

- **Biometrics at Sea System (BASS)** – BASS is a program led by the USCG that has led to increased prosecutions. BASS is currently installed on fifteen 110-ft cutters and seven 87-ft cutters that operate in the waters west of Puerto Rico and in southern Florida. The program collects fingerprints, a photograph, and biographic data, and sends this information to the DHS biometric database to determine if an individual poses a security threat. This allows the Coast Guard to quickly identify individuals who may have been previously been deported from the U.S. or who have active criminal warrants.

- **United States Visitor and Immigrant Status Indicator Technology (US-VISIT)** – Similarly, the US-VISIT program has grown and expanded its capabilities to capture fingerprints at its ports of entry in the U.S. and at Department of State consulates and visa centers around the world. Initially rolled out as a two-fingerprint process, DHS has evaluated the possible use of additional modalities, including facial recognition and iris matching, and has upgraded its collection technology to capture facial images and support ten-fingerprint capabilities. Collecting ten prints improves matching accuracy and the department’s ability to compare visitors against latent fingerprints provided by defense databases and the FBI’s Criminal Master File of known and unknown terrorists. The increased information provided by additional prints is not only more accurate, it also makes the process faster and enables agents to more quickly identify legitimate travelers who do not pose a threat.

**Challenges to collecting and sharing biometric data**
While there are many aspects of biometric identification that are going well along the U.S./Canada border, there are a few core challenges that present potential roadblocks for continued success. While the U.S. and Canada are committed to sharing biometric data, the information sharing process has not been seamless. Sharing information between the two nations requires navigating different regulatory environments. Both the

---

U.S./Canada Border Security Summit An Intelligence-Based Roadmap
U.S. and Canadian governments have strict privacy laws with significant requirements and restrictions that govern how personally identifiable information is shared and accessed. In order to move towards the Beyond the Border vision, some actions may require amendments or additional legislation in order for the U.S. and Canadian border agencies to more fully share biometric information. While CIC is working through these challenges to facilitate information sharing, regulatory constraints remain one of the largest barriers to information transfer.

Information sharing challenges are not limited to international agencies. Within the U.S., information sharing between different agency silos has been historically difficult. Federal agencies use different systems for information collection and have different purposes for the information they collect. This can make it difficult for agencies to process requests from other agencies for biometric information. In addition, agencies have not normally had the appropriate measures in place to facilitate information sharing. For example, a Government Accountability Office report indicated that, as of March 2011, DHS did not have an agreement in place to allow for the direct connectivity between the biometric systems for each agency, significantly increasing the time required to answer a request for biometric information.

There are several challenges related to resources that could impact the future results of biometrics programs. Biometrics requires personnel and technology resources to capture information. Collecting this information can be time and resource-intensive and requires trained personnel to operate equipment and understand biometric outputs. If current successful pilot programs along the border are expanded, additional personnel and resources will be required to collect information.

When it comes to biometric collection technology, better technologies will also need to be developed or deployed to meet the needs of the U.S./Canada border. While some programs are working to move to a capture that uses all ten of an individual’s fingerprints, eventually more programs will need to incorporate the ten-point capture, and potentially even more types of biometric modalities, to remain on par with current technology and support interoperability with international partners. Specific technology challenges also exist for capturing biometric information at less traditional points of entry where traditional collection approaches may not be applicable. It is particularly important to consider how feasible it is to collect biometric information along the open U.S./Canada border and how any increase in information collection in these areas might impact local commerce, as well as
the specific challenges posed by the winter weather and environment on the northern border. Cold, dry air results in stiff, dry fingerprint ridges that do not image well. Outdoor use in this environment may require relatively expensive specialized equipment to support effective collection of biometrics, including ultrasonic sensors equipped with heaters.

**The path forward – expanding and scaling biometric capabilities**

Expanding the use of biometrics and addressing challenges around information sharing, technology, and resource limitations will require a series of steps to enhance collaboration, testing of technologies, and data sharing. Collaboration is a key enabler for addressing some of these challenges. In Canada, the Biometrics Project at CIC has built privacy concerns and safeguards into their biometrics solutions to protect the data they collect, and has also designated the use of such information for immigration rather than intelligence purposes, making it easier for Canadian agencies to share information with their American counterparts – but also potentially limiting the purposes for which it can be leveraged. Part of addressing these privacy concerns is establishing strict enforcement mechanisms when dealing with vendors and service providers, as well as stringent standards to maintain and dispose of data. By establishing requirements for interoperability and quality assurance, the U.S. and Canada can also help to build the way for additional international partners to participate and encourage further extension of collaboration and information sharing efforts.

The ability to collect biometrics on behalf of other governments is an essential element of any collaborative partnership program and will be critical to avoiding duplication of effort. The U.S. and Canada have a timetable for establishing agreements which would help both countries identify dangerous actors and prevent them from travelling to Canada or the U.S., prevent individuals from assuming different identities between the two countries, identify those who have committed serious crimes or violated immigration law in the other country, and enable both countries to make informed decisions on visas, admissibility and other immigration benefits. US-VISIT is also moving forward with partnerships with Australia, New Zealand, and the United Kingdom to promote biometric information-sharing, with the hope of

**Biometrics at Sea**

Since its implementation in 2006, the Biometrics at Sea System (BASS) has led to over 900 prosecutions using the fingerprint data collected by the USCG. In Puerto Rico, there was a successful recovery of ammunition, money, and weapons that was based on information collected by the USCG in cooperation with CBP. Since its inception, illegal migration in the area has been reduced by 75%.
expanding relationships in China and elsewhere in the E.U. as well. Enhanced and continued collaboration through bilateral agreements, international working groups, and conferences is crucial, and will likely continue as individual countries expand their data collection and maintenance abilities.

While partnering with international stakeholders is one facet of improving biometric identification, the U.S. may also be required to implement interagency data-sharing plans that outline clear roles and responsibilities for sharing this information. US-VISIT maintains a repository of biometric information that has been collected since the aftermath of 9/11, and is now in the process of building a more robust network of information sharing throughout the U.S. that will allow agencies to know more about the people who are trying to enter the country. The network is used to service the biometric and identity requirements for ICE, as well as other federal homeland security and defense agencies; stakeholders in state and local law enforcement; and the intelligence and international communities. This network should spur increased collaboration among these stakeholders to execute their common missions. Continuing to build relationships among the interested agencies will be a key driver for developing a full biometric program in the U.S.

Testing and evaluating multimodal technologies to improve security and usability of future biometric technologies will also address several of the concerns raised around biometrics. These technologies include integrating facial recognition, iris scans, and other modality into existing programs, as well as focusing on technology advances that help establish a faster and more user-friendly biometrics collection process. Multi-modal biometric systems offer the benefit of increased population coverage, as incorporating the types of biometrics collected increases the probability that a given individual will be able to participate in at least one modality, thereby increasing the percentage of the population the system can serve. Another potential benefit of a multi-modal biometric system is improved accuracy through the combined use of multiple biometric inputs, known as the biometric fusion rule. This improved accuracy can be realized in the form of maintaining or reducing the False Reject Rate (FRR) while also maintaining a low False Accept Rate (FAR).

These efforts will require collaboration to develop more holistic technological solutions in which partners and agencies approach biometrics in a cohesive way to create an efficient and integrated system. A common interface for biometric output will need to be established in order for stakeholders to be able to understand and verify biometric data, rather than collecting new information that may already have been gathered by another agency. This will allow partners to avoid having to recheck data from multiple countries’ databases, which will save time and resources in an increasingly challenging budget environment.
Tools for border security: applying current and future technologies in an effective and efficient manner

Enhancing security through advanced technology
The use of technology on the U.S./Canada border has historically been fragmented and disaggregated with a strong emphasis on localized investment. This historic mindset has begun to transform in recent years to a holistic investment in technology that emphasizes the importance of collaboration, cooperation and information sharing. For the first time, the U.S. and Canada have a shared vision with both President Obama and Prime Minister Harper committed to taking responsibility for enhancing security and efficiency at and between ports of entry. Technological advances that facilitate effective and proactive observation have been vital in making national and binational pilot programs successful.

Committed to a binational enforcement effort, both Canada and the U.S. currently use technologies in several demonstrated U.S./Canada border security initiatives. These uses include detecting and classifying incursion, inspecting people and conveyances, managing risk, synthesizing data, identifying contraband, protecting personnel, and providing situational awareness. These technology uses are successfully enhancing the efficiency of security processes at and between ports of entry.

- **Mobile surveillance** – Between ports of entry, mobile surveillance systems have been increasingly used to successfully improve detection efficiency. Mobile Surveillance Systems consisting largely of mobile, relocatable radars and cameras have been piloted at a series of locations along the U.S./Canada border. Remote video surveillance systems deployed along the St. Claire and Niagara Rivers are operational and have been successfully implemented.

- **Non-invasive screening** – At ports of entry, new technologies are being developed and piloted to provide alternative, non-invasive ways to scan cargo. These non-invasive technologies utilize x-ray, gamma ray, and nuclear detection systems and software are valuable resources in decreasing inspection time while increasing detection and improving accuracy.

These technological innovations provide a glimpse of the U.S. and Canada’s recent achievements at and between ports of entry. The results of these programs can largely be attributed to pairing technological advancements with current efficiency gaps through information sharing and collaboration. Co-location and collaboration approaches pioneered by the OIC, RMCP, and the DHS Science and Technology Directorate have resulted in pilots and restructuring to break down the historically localized tactics. There has been an increase in information sharing through the movement towards a hub concept with a small number of common locations, which have translated current gaps into research and development efforts.

Challenges to implementing next generation technology
Despite these technological successes at and between ports of entry, binational initiatives face several implementation challenges to fulfilling the Beyond the Border strategy with current technologies.

- **Differentiated border environment** – There are specific difficulties posed by the U.S./Canada border that drive a differentiated approach to how border security is managed. At 5,500 miles, with highly varied terrain, wildlife, environments and weather, the border requires a collection of technologies and processes rather than any one-size-fits-all solution. Tailoring technology for the distinctive and varied environments of the U.S./Canada border requires forethought and a keen understanding of border locations. In particular, strategies that the U.S. has used on the southwest border with Mexico cannot be directly applied to the northern border with Canada without substantial changes in both technology and process.

- **Open border culture** – Furthermore, the “open border” culture between Canada and the U.S. creates surveillance challenges. Areas of the border region are populated by homes and towns, creating a need to protect the privacy and environment in which citizens live. The prohibition of fences creates substantial “clutter”, or false positives, on ground sensors and border cameras due to natural occurrences, such as wildlife crossing the border. These false positives are compounded by the fact that many border securing technologies can detect but not identify potential threats.

- **Scaling and expanding prototypes** – Another challenge faced by border officials trying to employ improved technologies is the need to move from test bed results to a holistic adoption of technologies.
Currently, there are many technologies being tested in small deployments across the border region. These test beds involve government collaboration, public-private partnerships, and other combinations of actors seeking to improve the tools and technology employed at the border. While this strategy allows the development of multiple technologies and allows border agencies to pilot potential solutions without committing significant resources, it does not prepare individuals for the changes in processes and culture that accompany technology adoption. Finding a method of taking successful test-bed solutions to a larger audience brings significant complications that border agencies must work to overcome.

• **Facilitation** – Canadian and U.S. border agencies also face the challenge of moving from technology specifically designed to stop threats to technology designed to facilitate trade and travel. This is particularly true in defining and measuring metrics to be used for decision-making. For example, the wait time for customs processing at borders is closely measured, but the total throughput time is not. This makes it difficult to establish a baseline for technology or process improvement for facilitation of trade and travel at border crossings.

Lastly, U.S. and Canadian border agencies are both living in a time of restricted budgets. This makes it more difficult to invest in border-securing or trade facilitating technologies, particularly on a transformational scale. Cost of technologies is a major consideration, especially for software developed from the ground up and not purchased as a commercial-off-the-shelf product. Many of the existing border security technologies, such as maritime radar and dual-band radios, are expensive, limiting available funds for new investments. Therefore, new technologies tested in test beds must show a positive impact on operations and high return on investment to be approved for use in large-scale operations. Technologies that drive efficiencies are also highly desirable due to their ability to drive down process costs.

**The path forward – shared, risk-based technology to build economies and enhance security**

To address the specific security challenges of the U.S./Canada border, both countries should build upon a "perimeter approach" to enhance security and support economic competitiveness. The path forward to move beyond the challenges includes addressing threats earlier via intelligence sharing and collaboration across and among a wide-range of U.S. and Canadian agencies at the national, state/provincial, and local levels. Co-habitation of intelligence/fusion centers – many of which successfully use automated technology platforms and solutions to support information sharing – has demonstrated to be useful in addressing threats early and bringing them to an appropriate law enforcement resolution.
Shifting to a risk-based approach that deploys the most effective inspection and scanning technologies to detect and prevent the entry of hazardous materials, goods, and terrorist weapons is another component of the path forward. Examples include advanced screening programs which ensure that containers that pose a potential risk for terrorism are identified and inspected at foreign ports before they are placed on vessels destined for the U.S.; mobile Non-Intrusive Inspection (NII) technologies which detect and interdict weapons, narcotics, currency, and other contraband hidden in commercial shipments; large-scale X-ray and gamma-ray imaging systems; radiation detection technology; portable and handheld devices; and “Green Lane” and trusted traveler programs.

Through the sharing of technology leading practices, U.S. and Canadian officials will continue to enhance U.S./Canada border security and support the need to facilitate the flow of legitimate trade and travel. Forums such as the U.S./Canada Border Security Summit provide U.S. and Canadian officials with opportunities to learn from their counterparts. Examples of such leading practices include:

- Tested technologies currently in use that support trade facilitation and reduce operational costs
- Innovative technologies that leverage mobile platforms and mobile surveillance programs
- Innovation Centers which collect and synthesize raw data in one central location; technology platforms that measure, monitor, and track supply chain security beyond the ports of entry
- Cost-effective IT investments that maintain current operations and improve efficiency, rather than introduce new capabilities
- Strategies for addressing organization and cultural changes that typically accompany the deployment of new technologies

In this era of austere budgets, it is even more important for U.S. and Canadian agencies to continue to build and sustain public-private partnerships that will enable the development of new technologies for border security. Creating an environment where agencies are willing to provide access to proprietary data and operations, and where private industry is willing to participate and invest in development at their own expense, can greatly reduce the need for government funding. These partnerships are most

**Electronic Chain of Customs Devices (ECOC)**

In January 2012, CBP and the DHS Science and Technology Directorate partnered to announce the piloting of Secure Transit Corridors. Under this pilot, Electronic Chain of Customs (ECOC) devices, electronic locks that maintain records of opening and travel, will be used to monitor cargo door tampering from point of loading to unloading. The initiative seeks to deploy new technology and infrastructure to help secure land cargo entering the U.S. from Canada and Mexico, and confirm cargo integrity to expedite border crossings. Alarms will be routed to CBP’s Laboratories and Scientific Services Tele-Forensics Center for dispatching and will be supported by capabilities for tracking and monitoring and global communications.

**Mobile VACIS**

CBP has begun conducting examinations with Non-Intrusive Inspection (NII) equipment. NII has the potential to identify contraband without opening containers by providing “vision” into cargo through low-energy X-ray or low-energy gamma radiation. Mobile technology can also expedite inspections by allowing cargo exams on location, rather than taking the container to an inspection facility.

- As part of the NII initiative, CBP has implemented four types of Vehicle and Cargo Inspection System (VACIS®) gamma-imaging tools:
  - VACIS®II – Semi-permanent version designed for inspection of motor vehicles and cargo containers at CBP ports of entry
  - Mobile VACIS® – Truck-mounted version designed for high-portability inspection of motor vehicles and cargo containers
  - Rail VACIS® – Fixed version designed specifically for installation along railroad rights of way, for the inspection of railroad cars
  - Pallet VACIS® – Fixed pallet system designed for inspection of pallets, boxes or crates
appropriate for areas where technology improvements are mutually beneficial to the government and industry. As a result, private industry finds a market for their new products and/or benefits from reduced processing times and improved facilitation and public entities get access to breakthrough technologies at a lower cost of entry. Benefits of effective partnerships include improved ability to monitor and facilitate a secure international supply chain; increased affordability of technologies; leveraging leading thinking via academic centers of excellence; and evidence of tested initiatives in the private sector that can be transferred to border operations. Critical to these partnerships is developing a framework for how agreements can be structured, formalizing mechanisms for entities to work together, involving academic centers of excellence as clearinghouses, and obtaining approvals for outside companies to get access to public resources and operational environments.

Improved technology and collaboration create a framework for the “port of the future”, a port which emphasizes facilitation as well as security. This port of the future could be built through partnerships between the public and private sector, with the goals of strengthening regional economies, improving international trade, promoting tourism, and spurring community development by making international ports of entry as efficient and effective as possible. Specifically, ports of the future accomplish the following:

• Expedite the movement of goods via advanced screen before containers are loaded (CBP’s Container Security Initiative is one example). These ports use mobile devices to screen high risk/unknown cargo. In addition, “Green Lanes” accelerate the flow of legitimate goods for low risk cargo at ports of entry.

• Facilitate the flow of passenger processing (CBP’s NEXUS program is one example). Future improvements will include simplified oversees airport screening processes to address threats and streamline the disembarkment process.

• Address current infrastructure, rather than simply redesigning bridges and roads, to more effectively manage traffic. The focus needs to be on a combination of fast lanes for trusted travelers, separate lanes for non-trusted travelers, and other lanes for pre-processing.

• Leverage technology, automation, and innovation to improve operational performance.

• Address environmental sustainability, include alternative energy sources or electric drives, conserve water and other precious resources, leverage radiant heating and cooling panels, reduce tail pipe carbon by decreasing automobile idle time, and protect officers from inclement weather.

Since 9/11, U.S. and Canadian Governments have invested significantly in technology approaches and solutions designed to enhance the security of both the U.S./Mexico and U.S/Canada borders. Hundreds of pilot programs have been funded to address a range of border security challenges. The challenge today is to identify those cross-border pilot projects that have been effective and expand upon them. The emphasis should be on improving efficiency, rather than developing new capabilities; reducing false alarms in which technology is unable to differentiate between potential threats and wildlife, inclement weather, etc.; aligning technologies to specific threats; ensuring interoperable communications/ IP communications; leveraging smartphone technologies; and organizing products into portfolios.

It is understood that technology must balance the dual needs for security and facilitation. As such, it is imperative to think beyond wait times and reconsider how success is measured and what role technology can play.
**Presenters**

**DSI and Deloitte** would like to thank the following distinguished experts for presenting at the Summit:

**Nelson Balido**  
President, Border Trade Alliance  
*Current Border Issues: An Update from Capitol Hill*

**Mark S. Borkowski**  
Assistant Commissioner, Office of Technology Innovation and Acquisition, U.S. Customs and Border Protection  
*Meeting the Challenges of Securing and Managing the US - Canadian Border Through Pre-Existing Technology to Meet CBP’s Mission*

**Tammie Bustamante**  
Project Manager, Biometrics at Sea Systems, United States Coast Guard  
*Bio Metrics at Sea: Demonstration and Discussion – Collection, and Integration for the U.S Coast Guard*

**Richard Comerford**  
Regional Director General, Southern Ontario Region, Canada Border Services Agency  
*CBSA’s Focus on Targeting High-Risk People and Goods Before They Reach the Border*

**Anh Duong**  
SES, Director for the Borders and Maritime Security Division, Science and Technology Directorate, DHS  
*Technologies for “Beyond the Border”: Detection Against Land/Air/Maritime Threats and Cargo Supply Chain Security*

**Stephanie Kirkland**  
Director General, Biometrics Project Office, Citizenship and Immigration Canada  
*Canadian Multi Biometrics Applications for Immigration and Border Security*

**Randy Gallegos**  
Chief Border Patrol Agent, Detroit MI  
*Implementing a Strategy Focused on Information, Integration and Rapid Response for the Detroit Sector*

**William Hayes**  
Deputy Special Agent in Charge of Homeland Security Investigations, Michigan and Ohio ICE  
*ICE’s Role in Border Security: Investigation, Interdiction and Security for the U.S./Canadian Border*

**James King**  
Technician, Biometrics at Sea Systems, United States Coast Guard  
*Bio Metrics at Sea: Demonstration and Discussion – Collection, and Integration for the U.S Coast Guard*

**Bob Martin**  
Hardware, Biometrics at Sea Systems, United States Coast Guard  
*Bio Metrics at Sea: Demonstration and Discussion – Collection, and Integration for the U.S Coast Guard*
Marc Mes
Director, Maritime Security, Canadian Coast Guard
*Canadian Coast Guard’s Contribution to Information-Driven Maritime Security Activities*

Robert Mocny
Director, US-VISIT, DHS
*Innovative Multimodal Biometric Technology from US-VISIT*

Tracy North
Deputy Assistant Director of the Intelligence Services Branch, Directorate of Intelligence, FBI
*FBI: An Intelligence-Driven, Threat-Focused Approach to Border and Homeland Security*

Joe Oliver
Chief Superintendent, Director General for Border Integrity, Royal Canadian Mounted Police
*Beyond the Border Action Plan: Integrated Cross-Border Law Enforcement*

RDML Michael Parks
Commander, 9th District, United States Coast Guard
*USCG and CCG MARITIME Operations: A Multi Layered Approach to Security*

Jim Phillips
President, Canadian/American Border Trade Alliance
*Coordinated Clearance - Point of Determination End State of the Beyond the Border Perimeter Strategy*

Captain W. Thomas Sands
*Micinigan’s Homeland Security Framework: Initiatives and Challenges*

Inspector Harvey Seddon
Officer in Charge of Border Integrity, “O” Division, Royal Canadian Mounted Police
*Mission Specific Needs: RCMP’s “O” Division Perspective*

Marci Sutton
Software & Training, Biometrics at Sea Systems, United States Coast Guard
*Bio Metrics at Sea: Demonstration and Discussion – Collection, and Integration for the U.S Coast Guard*

Dr. Andrew L. Vallerand
Director, Public Security Technical Program (PSTP), DRDC Centre for Security Science, Canada
*Canada’s PSTP: Building SAT-Based Capabilities to Identify and Stop Terrorist and Criminal Activity in the Border and Transportation Security Domains*
About DSI
The Defense Strategies Institute (DSI) is a premier non-partisan Veteran Owned Small Business designed to assist in advancing the mission critical goals of the United States’ Military and Government. Through our high level educational and training summits, conferences, and symposiums we are able to reach across all offices and departments in a fair and balanced manner. We bring together the mission relevant representatives in our neutral forums in order to foster the necessary discussions and debates to help them achieve efficient and effective mission success.

About Deloitte Federal
With more than 6,000 practitioners dedicated to serving the Federal Government, including 75 former senior government executives, Deloitte takes pride in helping our clients get big things done. Deloitte’s knowledge of the Federal Government and technical experience is virtually unparalleled. We serve all 15 U.S. Cabinet-level agencies and 10 out of 25 of Deloitte’s top clients are Federal agencies or departments. Our Federal team members have worked in both the public sector and private industry, which means that they can leverage leading practices from all sectors to help achieve tangible results. From headquarters to the back office to the front line, we work side by side with clients to design and implement their most strategic, complex initiatives to achieve results for the American people.

About the Summit
The U.S./Canada Border Security Summit took place from April 3-4, 2012 in Dearborn, MI. The Summit benefited the following nonprofit foundations through DSI’s charitable contributions:

United States
• The Roger L. Von Amelunxen Foundation: Supporting employees and families of Customs and Border Protection (CBP) & Immigration and Customs Enforcement (ICE)
  Roger L. Von Amelunxen was a Customs Patrol Officer who was slain in 1980. His family started the Foundation in 1982 in memory of their son. The Foundation is a non-profit and incorporated in the State of New York. The Foundation’s purpose is to provide financial assistance to U.S. Customs and Border Protection and Immigration and Customs Enforcement employees and their immediate families nationwide. The Foundation has disbursed over $5.2 million to what is now CBP and ICE employees and their families. http://www.rogerfoundation.org/

Canada
• The RCMP Foundation – National Remembrance Fund: In memoriam to fallen RCMP employees.
  The Royal Canadian Mounted Police (RCMP) occupies a unique position in the world as a National, Federal, Provincial and Municipal policing body, providing policing service to all Canadians. The job of an RCMP officer is one that requires great sacrifice and dedication. Everyday thousands of officers across Canada put their lives on the line to serve and protect in their communities. Sadly for some officers, being in the line of duty has meant giving the ultimate sacrifice. Since the 1870s, a total of 230 offices from the RCMP have lost their lives in the line of duty. The National Remembrance Fund is dedicated to honoring the work of those fallen RCMP employees across Canada and ensuring that the significance of their sacrifice will never be forgotten. http://www.rcmp-f.ca/national-remembrance-fund/
U.S./Canada Border Security Summit: An Intelligence-Based Roadmap
Contacts
For additional information regarding the content of this Post Summit Report, please contact:

Bob Jacksta
Deloitte Financial Advisory Services LLP
+1 571 227 8022
rjacksta@deloitte.com

Norman Montgomery
Deloitte Consulting LLP
+1 571 814 7630
nmontgomery@deloitte.com

Kwasi Mitchell
Deloitte Consulting LLP
+1 571 814 7801
kwmitchell@deloitte.com

Lauren Ross
Deloitte Consulting LLP
+1 571 882 8259
laurross@deloitte.com

In Canada:

Kelly McInnis
Deloitte Canada
+1 613 786 7586
kmcinnis@deloitte.ca

Contributing authors

Maya Chenault, Deloitte Consulting LLP
Joni Clegg, Deloitte Canada
Bridget Venne, Deloitte Consulting LLP
Amy Shields, Deloitte Consulting LLP
Jeyson Florez, Deloitte Consulting LLP
Sean Graber, Deloitte Consulting LLP
Sam Sholander, Deloitte Consulting LLP
Caitlin Souther, Deloitte Consulting LLP
Danielle Vildostegui, Deloitte Consulting LLP

For more information on Defense Strategies Institute, contact:

Lisa Madison
Director, Communications
+1 347 732 5326
lmadison@dsgroup.org


This publication contains general information only and is based on the experiences and research of Deloitte practitioners. Deloitte is not, by means of this publication, rendering business, financial, investment, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte, its affiliates, and related entities shall not be responsible for any loss sustained by any person who relies on this publication.

Copyright © 2012 Deloitte Development LLC. All rights reserved.
Member of Deloitte Touche Tohmatsu Limited