



ARCHIVED - Archiving Content

Archived Content

Information identified as archived is provided for reference, research or recordkeeping purposes. It is not subject to the Government of Canada Web Standards and has not been altered or updated since it was archived. Please contact us to request a format other than those available.

ARCHIVÉE - Contenu archivé

Contenu archivé

L'information dont il est indiqué qu'elle est archivée est fournie à des fins de référence, de recherche ou de tenue de documents. Elle n'est pas assujettie aux normes Web du gouvernement du Canada et elle n'a pas été modifiée ou mise à jour depuis son archivage. Pour obtenir cette information dans un autre format, veuillez communiquer avec nous.

This document is archival in nature and is intended for those who wish to consult archival documents made available from the collection of Public Safety Canada.

Some of these documents are available in only one official language. Translation, to be provided by Public Safety Canada, is available upon request.

Le présent document a une valeur archivistique et fait partie des documents d'archives rendus disponibles par Sécurité publique Canada à ceux qui souhaitent consulter ces documents issus de sa collection.

Certains de ces documents ne sont disponibles que dans une langue officielle. Sécurité publique Canada fournira une traduction sur demande.

A MAGAZINE ABOUT THE CANADA PUBLIC SAFETY INFORMATION NETWORK

IJI@WORK

SUMMER 2004, Vol. 3 ISSUE 1

USING **BIOMETRICS** TO FIGHT TERRORISM



Interoperability:
THE NEXT EVOLUTION
OF IJI IN CANADA

PARTNERS IN
PROFILE

QUEBEC AND SASKATCHEWAN
CONNECT TO OMS

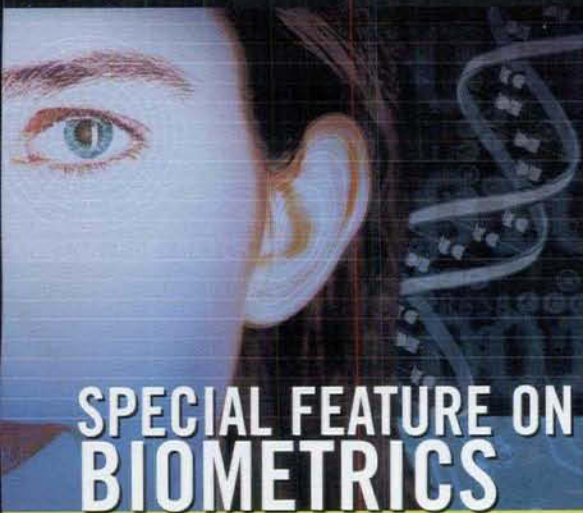
BC AND ONTARIO
LEIP INTO ACTION

Canada

CONTENTS

3 Foreword
A Message from the
Honourable Anne McLellan

4 A Note from the
Editor-In-Chief



SPECIAL FEATURE ON BIOMETRICS

- 14** Identifying the possibilities:
Biometrics in Canada
- 16** Q&A with Raj Nanavati on
biometrics standards development
- 18** Looking at the bigger picture:
Canada's new National Security Policy
- 20** Put to the test:
Does facial recognition measure up?
- 22** Charting new waters:
The Seafarers' Identity Document
- 24** Iris recognition
CANPASS Air simplifies border
clearance for frequent flyers
- 26** Putting the pieces together:
Making real-time
identification a reality

INTEROPERABILITY IN PROFILE

5 Interoperability
Charting the next phase
in the evolution of
integrated justice
information in Canada



9 Are you
receiving?
Tuning into the
challenges of radio
interoperability

12 For the asking
The RCMP's
Integrated
Query Tool

PARTNERS IN PROFILE

LEIPs and bounds

A "just do it"
attitude yields rapid
progress for IJI in
Ontario and BC

28



Connecting partners in Quebec and Saskatchewan

Correctional Service
Canada's Offender
Management System

32



35

Getting it done
New Brunswick is making
strides in the realm of IJI

38 Highlights from the CACP forum on
information sharing and interoperability

41 Highlights from the Strategies for Public
Safety Transformation 2004 conference
on technology and counter-terrorism



A common will to connect

Update on partnerships
and Canada-U.S.
public-safety efforts

43

ABOUT IJI@WORK

IJI@Work is published by the Integrated Justice Information Secretariat of Public Safety and Emergency Preparedness Canada. Opinions expressed in this publication do not necessarily reflect the views or opinions of the Public Safety and Emergency Preparedness Canada.

ISSN 1703-0129
Vol. 3 Issue 1

© Her Majesty the Queen in Right of Canada, represented by the Solicitor General of Canada (Minister of Public Safety and Emergency Preparedness), 2004. All rights reserved.
Printed in Canada

EXECUTIVE DIRECTOR

Greg Wright

EDITOR-IN-CHIEF

Eleanor Willing

CONTRIBUTORS

Patrick Gant,
thinkit communications

Andrew Kirkwood,
Stiff Sentences Inc.

GRAPHIC DESIGN

Accurate Design and
Communication Inc.

PHOTOGRAPHY

tecklesphoto.com

Articles may be reprinted in whole or in part with credit to Public Safety and Emergency Preparedness Canada.

Letters to the editor, suggestions for articles and contributions are welcome.

Material submitted may be edited for style and length. All contributors must include an email address and daytime phone number.

Address all correspondence to:

IJI@Work
Public Safety and Emergency
Preparedness Canada
Integrated Justice Information Secretariat
340 Laurier Ave. West
Ottawa, ON K1A 0P8
Telephone: (613) 991-4279
Fax: (613) 991-3306
Web: www.psepc.gc.ca
Email: ijis-sij@psepc-sppcc.gc.ca

FOREWORD



A Message from The Honourable Anne McLellan, Deputy Prime Minister and Minister of Public Safety and Emergency Preparedness Canada

As Deputy Prime Minister and Minister of Public Safety and Emergency Preparedness, I am pleased to have the opportunity to provide greetings to the readers of *IJI@Work*.

On December 12, 2003, the Prime Minister announced the creation of a new Department of Public Safety and Emergency Preparedness Canada (PSEPC). The Department brings together the core functions of security and intelligence, policing and enforcement, corrections and crime prevention, border services and integrity, immigration enforcement, and emergency management.

The creation of PSEPC, along with its agencies, is a fundamental component of the Government of Canada's efforts to better secure Canada's public safety and security. PSEPC is working with its partners in all levels of government, and all sectors of society, to build a safer, more secure Canada that respects the civil liberties of a diverse democracy and the collective security expected by our citizens.

These partnerships are essential to our work, and therefore, must be nurtured by an environment that encourages an open exchange of information and ideas. Through this publication, *IJI@Work*, the Integrated Justice Information Secretariat continues to play this important role in support of public safety.

Citizens, interested stakeholders, Canadian Public Safety Information Network (CPSIN) partners, and front-line workers in criminal justice and public safety can take pride in Canada's integrated justice information achievements to date—many of which have been profiled in this publication. Each accomplishment is a step forward for public safety and criminal justice in Canada and abroad.

I encourage you to continue to work with your domestic and international partners to maintain and enhance the security of Canadians.

A handwritten signature in cursive script that reads "Anne McLellan".

The Honourable A. Anne McLellan, P.C., M.P.
Deputy Prime Minister and
Minister of Public Safety and Emergency
Preparedness Canada





A NOTE FROM THE EDITOR-IN-CHIEF

Change is a constant force in nature—partners in the integrated justice information community are not immune from this fact. In the span of time between this fourth issue of *IJI@Work*, and its predecessor, we have seen some very important changes in the Government of Canada's public safety portfolio, including the creation of our new department, Public Safety and Emergency Preparedness Canada, and the launching of Canada's first-ever integrated National Security Policy.

These changes are part of a much wider set of developments that are taking place in Canada's public safety and criminal justice communities. Interoperability and biometrics are being pursued through various undertakings across government, offering tremendous new potential for information sharing in a controlled, secure environment.

Recognizing the importance of these changes, we've devoted a significant portion of this publication to highlight the efforts underway across Canada right now. Each article reveals how important breakthroughs hold the promise of advancing our collective goal of integrated justice information.

The Canada Public Safety Information Network derives much of its strength from the achievements of its partners who are seeking better ways to work and share with each other. That's why this issue of *IJI@Work*, also highlights some of the key achievements of the provinces, including: a Correctional Service Canada agreement with Quebec, Saskatchewan and British Columbia; law-enforcement collaboration efforts in Ontario and British Columbia; as well as highlights from recent conferences on information sharing, technology and counter-terrorism.

As always, I am interested to hear your impression about *IJI@Work*. Be sure to send us an email at ijis-sijj@psepc-sppcc.gc.ca. Your feedback will help shape future issues of this magazine.

Eleanor Willing

Eleanor Willing
Editor-in-Chief, *IJI@Work*

INTEROPERABILITY
IN PROFILE

INTEROPERABILITY IN CANADA:

Charting the next phase in
the evolution of integrated
justice information

INTEROPERABILITY IS A TERM THAT IS QUICKLY BECOMING PART OF THE LEXICON OF THE PUBLIC SAFETY, CRIMINAL JUSTICE AND INFORMATION-TECHNOLOGY COMMUNITIES. AND INTEREST IN THIS WORD AND ITS MANY APPLICATIONS IS NOT LIMITED JUST TO CANADA. A KEYWORD SEARCH FOR INTEROPERABILITY USING GOOGLE (A POPULAR INTERNET SEARCH ENGINE) GENERATES MORE THAN TWO MILLION INDIVIDUAL HITS, WITH LINKS TO CRIMINAL JUSTICE, TECHNOLOGY AND SECURITY ORGANIZATIONS WORLDWIDE. YET A STANDARD DEFINITION OF THE TERM—THE ABILITY OF SOFTWARE AND HARDWARE ON MULTIPLE MACHINES FROM MULTIPLE VENDORS TO COMMUNICATE—ONLY HINTS AT THE REAL POTENTIAL OF INTEROPERABILITY AND OF THE CHALLENGES PRESENTED IN ITS PURSUIT.

No country has yet achieved full interoperability or all-encompassing information sharing, but that could soon change. Thanks to the efforts of partners in the Canada Public Safety Information Network (CPSIN), the stage is set for improved interoperability among Canadian criminal justice and public safety organizations—in effect, opening the door to the next phase in the evolution of integrated justice information in this country.

In 2005, CPSIN's five-year Action Plan will come to a close, having achieved its key objectives. This will serve as an important foundation on which future integrated justice information initiatives—and indeed interoperability across the public-safety sector—will be enhanced.

WHAT IT MEANS TO CITIZENS

Canadians will soon be able to see the results for themselves on their streets, at airports, and in the courts (among many other public places). For example, police will be able to readily exchange criminal justice information with their counterparts in corrections and parole, using common data standards and adhering to a common dictionary of terms, descriptions and offences related to criminal justice cases. Eventually, courts will be able to access information generated by correctional organizations and parole boards, again adhering to common data standards and a common data dictionary. Already, Customs can read a licence plate number on a vehicle at a border crossing and know right away whether the police are looking for that vehicle. The potential public safety applications

THANKS TO THE CANADA
PUBLIC SAFETY INFORMATION
NETWORK, THE STAGE IS SET FOR
IMPROVED INTEROPERABILITY AMONG
CRIMINAL JUSTICE AND PUBLIC
SAFETY ORGANIZATIONS

ENHANCING PUBLIC SAFETY IN CANADA

The Government of Canada has responded to the public safety challenge by:

- creating the new Department of Public Safety and Emergency Preparedness, improving coordination and bringing together vital services and responsibilities under a single federal Minister;
- announcing a comprehensive Public Safety and Security Information Sharing and Interoperability project to address interoperability gaps and achieve secure, effective communications across all organizations that have significant public safety and security responsibilities;
- establishing the Canada Border Services Agency, integrating several key functions previously spread across three organizations—the Customs Program from the Canada Customs and Revenue Agency; the Intelligence, Interdiction and Enforcement Program from Citizenship and Immigration Canada; and the Import Inspection at Ports of Entry Program from the Canadian Food Inspection Agency; and
- launching Canada's first-ever integrated National Security Policy, ensuring a coordinated effort among domestic and international partners to address threats to Canadian national security.

INTEROPERABILITY IN PROFILE

are endless and the ramifications point to improved safety and security for all Canadians.

Interoperability and new information-sharing possibilities will not manifest themselves overnight. Rather, they will take time to achieve. More work has to be done to achieve a fully interoperable environment and an integrated flow of information across the public safety community. Among the initiatives that are currently being assessed in this regard is one that will enable partners to exchange secret-level information across a secure network.

A NEW PROJECT AIDED BY A NEW DEPARTMENT

Indeed, there is much excitement within the IJI Secretariat about the new Interoperability project, launched in May 2004. Its task over the subsequent 18-months is to develop a comprehensive vision and strategic design for achieving a sustainable interoperable environment that will serve the public safety interests of the Government of Canada. This project aims to address specific legal and policy challenges, such as respecting the privacy rights of the individual.

The need to get key agencies involved in the Interoperability Project was aided in part by the creation of the new department, Public Safety and Emergency Preparedness Canada (PSEPC).

This department will be leading the work on interoperability, conducting consultations and providing updates to public safety stakeholders. The project team is already focused on its first milestone—a progress

report for the federal Cabinet, due in the fall of 2004, that will identify the most pressing interoperability priorities.

FINDING AN AFFORDABLE SOLUTION

Carrie Hunter (Director, Interoperability Division) likes to refer often to a sign affixed to her bulletin board: "If we can't afford the solution, then it's not a solution." That's the essence of the challenge at hand, she explains. "It's a reminder not only to our suppliers, but to those of us in government who are working on interoperability and other integrated justice information-related activities that we have to be practical in what we're doing."

As Director of the Integrated Justice Information Secretariat's Interoperability Division, Hunter wants to ensure that interoperability does not become an information-technology project with a budget as big as its promises. Far from it: "We want to find a way to achieve our goals in a way that's as painless and as cost-efficient to citizens as possible," she says.



CARRIE HUNTER, DIRECTOR,
INTEROPERABILITY DIVISION,
IJI SECRETARIAT

"If we can't afford the solution, then it's not a solution."

“Up until now, solutions have generally been piecemeal, conducted in an ad-hoc manner and on a department-by-department basis. We lacked an overarching solution that could serve all of the Government of Canada.”

But finding an inexpensive route is only the start of the work within this new project. “We also want to encourage significant changes in information management and technology (IM/IT) business practices within the Government of Canada,” she explains. “In doing so, we’re striving to create a new environment where interoperability can influence the way we buy and what we buy, with respect to new technologies.”

NON-INTEROPERABILITY

Hunter contends, however, that this project will influence the public safety community within government and beyond. Too many information-technology systems within government exist in a state of non-interoperability—monolithic processes and structures unable to provide a meaningful level of information exchange with systems in other departments or jurisdictions. “We need the capacity to easily permit or stop information flows, when circumstances and the law dictate,” she says, “this is important as we continue to address ever-changing public safety challenges.”

There are a host of reasons that caused non-interoperability to become so pervasive across government—age, design and outdated functions of many IM/IT systems, for example—but there are also business reasons as well.

Hunter cites inherent federal procurement practices and competitiveness among suppliers as key barriers to interoperability. “We’ve discovered that interoperability isn’t a prominent

evaluation criterion used by Public Works and Government Services Canada in deciding on who will be the successful bidder on a contract,” she says. “We’d like to see that change.”

With respect to suppliers, she notes that “there’s a tendency among some, presumably for reasons of competitiveness, to create closed systems so that their client base remains loyal to their products.” Users encounter the effects of this every day, from databases that cannot share data, to documents that cannot open on computer systems in other offices where different software is being used. As a result, time is wasted finding work-around solutions—or worse—information exchange between some partners simply doesn’t occur.

Interoperability isn’t a solution that can be purchased by simply buying new equipment or new software. Rather, achieving it will hinge on changing many practices that characterize the way business is conducted in federal departments, including the way that equipment and technology are procured.

To address these kinds of issues, the Interoperability Division is calling on information-technology suppliers to join a voluntary working group to study ways to ensure their



products have built-in interoperability. Hunter is encouraged by the response she’s received from suppliers and expects the working group will start holding its first meetings by mid-2004.

AN END TO PIECEMEAL SOLUTIONS

Attempts to date at solving interoperability have also created problems, Hunter explains. “Up until now, solutions have generally been piecemeal, conducted in an ad-hoc manner and on a department-by-department basis. We lacked an overarching solution that could serve all of the Government of Canada.” The new Interoperability Project, led by Mark Bornais (Project Director), will serve to address this—not only due to the broad mandate of the department in which it resides, but also because the scope of its work has been extended beyond Canada’s criminal justice system to include other public safety organizations.

“What we’re saying,” Hunter adds, “is that we’re quite willing to work with other organizations—from public safety to national security—to help find out what’s preventing them from achieving full-scale interoperability with their partners.”

INTEROPERABILITY IN PROFILE

MAKING A CASE FOR A COMMON APPROACH

To illustrate the need for a common federal approach to interoperability, Hunter cites a case study. During 2002–2003, the former Canada Customs and Revenue Agency was working with its counterparts in the United States on an information-sharing system to provide authorities with advance passenger information on all in-bound flights into the United States. Canada's role in this was to develop a system that could collect information from airlines and enable security screening of passengers before they arrived. Meanwhile, the RCMP, CSIS and Transport Canada were considering a similar initiative proposed under the *Public Safety Act*. In this instance, information would be collected for use at airports to identify criminals and suspected terrorists who might attempt to board an aircraft.

Overlap between the two proposed IM/IT systems was remarkable—all but three data fields were identical. "Different areas of our organizations were involved with these systems," Hunter explains.

"Happily there was discussion and agreement on an efficient way to serve both purposes." Any potential for overlap or over-spending can be avoided, she adds, "by ensuring that all information-technology projects related to information sharing and interoperability are coordinated and that linkages are understood."

Granted, these are still early days for interoperability in the new department. The Interoperability Project has just started its work—a task that is best summed up as a scouting and research mission to provide the Government of Canada with a clear set of options from which to choose. Concludes Hunter: "we can't presume what the outcome will be of this assignment, but what we can be sure of is that interoperability will define how the Canada Public Safety Information Network will continue to evolve and grow over the next several years and well into the next decade."

The Interoperability Project is best summed up as a scouting and research mission to provide the Government of Canada with a clear set of options from which to choose.



INTEROPERABILITY
IN PROFILE

ARE YOU RECEIVING?

TUNING INTO THE CHALLENGES OF RADIO INTEROPERABILITY

IT'S OFTEN NOTED THAT CRIMINAL ACTIVITIES, NATURAL DISASTERS AND TERRORIST ACTS HAVE NO REGARD FOR JURISDICTIONAL BOUNDARIES. AND THAT MAKES IT IMPERATIVE FOR PUBLIC-SAFETY AGENCIES TO COMMUNICATE ACROSS THOSE BOUNDARIES—SEAMLESSLY AND IMMEDIATELY.

ANDRÉ LAFLÈCHE AND FRANCINE BOUCHER ARE PART OF A TEAM AT THE RCMP DEDICATED TO ENABLING EXACTLY THAT KIND OF COMMUNICATION THROUGH *RADIO INTEROPERABILITY*: PROVIDING LAW-ENFORCEMENT AND OTHER ORGANIZATIONS WITH THE TOOLS TO COMMUNICATE IN REAL TIME ACROSS ALL KINDS OF BORDERS—OPERATIONAL AND GEOGRAPHICAL ALIKE.

THROUGH A PILOT PROJECT CURRENTLY UNDERWAY IN ONTARIO'S WINDSOR AREA, LAFLÈCHE, BOUCHER AND THEIR COLLEAGUES HOPE TO GAIN A CLEAR, LONG-TERM UNDERSTANDING OF WHAT INTEROPERABILITY REALLY REQUIRES.

KELOWNA, BC COMMUNICATIONS TOWER SHARED BY RCMP, NAV CANADA AND TELUS.

PHOTO COURTESY OF DAVE PATTERSON, RCMP

INTEROPERABILITY IN PROFILE

A MULTI-FACETED CHALLENGE

The pursuit of radio interoperability is complicated by the fact that jurisdictional boundaries exist at many levels. Multiple agencies may operate within a single metropolitan setting—their ‘jurisdictions’ defined by role and mandate. They may operate on opposite sides of city limits, along provincial boundary lines, and even along the international border between Canada and the U.S.

It is in fact this latter case that led the RCMP to establish its radio interoperability team in the first place. At the summer 2002 meeting of the Canada-U.S. Cross-Border Crime Forum, it was agreed that agencies on both sides needed the freedom to communicate operational information in the interest of public safety.

André Laflèche—Senior Systems Project Manager of Mobile Communications Services at the RCMP—was tasked with defining interim solutions and developing a long-term interoperability strategy.

“In a city like Ottawa,” Laflèche explains by way of example, “it’s relatively simple for agencies operating locally—the RCMP and Ottawa Police, for instance—to sit down and work out an agreement to share communications. One has federal responsibilities, the other municipal, but they function at virtually the same level and cover virtually the same territory. And in fact this is what they’ve done, establishing a General Duty Protective Policing arrangement to support each other. But when you look across the Canada-U.S.

border things become more complicated, because now you’re talking about creating *international* agreements, which are necessarily more intricate—and which agencies don’t have direct authority to negotiate on their own.”

Laflèche says that while he and his team had originally believed such agreements needed to be operational in nature, that proved far too complicated in practice. “All these agencies—police, customs, border patrol—have their mandates and their ways of working,” he says. “To try to define those in detail—or *redefine* them—in the context of radio interoperability is simply too big a task.”

Instead, Laflèche has determined the best approach is to isolate and concentrate on communications issues: who needs to talk to whom, and under what conditions. “Of course, you have to be operationally aware,” he’s quick to add. “All of this always comes back to front-line requirements.”

THE QUESTION OF TECHNOLOGY

Laflèche observes that it is technically feasible today for many radio systems to intercommunicate in sophisticated and effective ways. But he notes that what’s good for today isn’t necessarily good for tomorrow.

“We’re between two paradigms,” he remarks, “the analog and the digital. New technologies, digital technologies, give you a lot of freedom to divide and subdivide a given frequency into controlled channels. So

you gain flexibility and functionality. But at the same time, digital technologies are a lot more complex than analog, and that—combined with a lack of standardization—makes them more difficult to integrate.”

Not surprisingly, Laflèche is convinced that digital solutions will prevail in the long term—especially because they can support both voice and data communications.

“But for now,” he says, “agencies understandably want to get as much life out of their legacy systems as they possibly can. So you have a mixture of technologies at work. To achieve interoperability in the near term you have to take a tactical, pragmatic approach.”

It’s exactly such an approach that Laflèche and his team have taken to their project in Windsor. However, before describing that work in greater detail, there’s one more factor of radio interoperability to consider: spectrum management.

WHAT’S THE FREQUENCY?

Laflèche’s colleague, Francine Boucher, is a Senior Systems Engineer and Manager of the Radio Spectrum Management Section of the RCMP’s Mobile Communications Services. She notes that the radio spectrum in Canada and the U.S. is almost fully assigned.

“It’s not an easy process for spectrum-licensing bodies to open up new bands,” she says. In Canada, that body is Industry Canada; in the U.S., the responsibility is

“New technologies, digital technologies, give you a lot of freedom to divide and subdivide a given frequency into controlled channels.”

INTEROPERABILITY IN PROFILE

shared between the National Telecommunications and Information Administration (NTIA) and U.S. Federal Communications Commission (FCC). "They have to apply to the International Telecommunications Union (ITU), which convenes just once every three years at the World Radio Conference. So these bodies have to be very careful and well-considered about how they assign the parts of the spectrum that are available."

This can make cross-border communications arrangements even more challenging to negotiate.

"If you have a Canadian police force that wants to open up its radio frequency to a U.S. counterpart," Boucher explains, "there may already be someone who has licensed that same frequency for another purpose on the other side of the border, and vice-versa. So how do you work out the solution?"

Phuong Vu manages Mobile & PCS Spectrum Engineering for Industry Canada. He says his department is certainly committed to overcoming these kinds of hurdles, and is working with NTIA and the FCC to streamline the authorization process for spectrum allocation along the border.

"We held a National Public Safety Radio Communications conference in 2002 to try to define the issues," Vu says. "We're very interested in improving radio interoperability, and we recognize that spectrum is part of the equation."

That said, he notes that what's most important to develop at this stage is some kind of national plan—a strategy for radio interoperability that Industry Canada can draw upon to establish concrete priorities for spectrum management in the future.

The foundation for such a strategy is being built right now in Windsor.

A PRACTICAL CASE STUDY

Windsor is in many respects an ideal location for studying radio interoperability at work. Located on a peninsula in southwestern Ontario—on the border with the

"What's most important to develop at this stage is some kind of national plan—a strategy for radio interoperability that Industry Canada can draw upon to establish concrete priorities."

United States—it presents a relatively contained environment in which agencies such as the Windsor police, the Ontario Provincial Police, the Canada Border Services Agency, the U.S. Border Patrol and U.S. Customs operate.

For this reason, the Windsor area already serves as an IBET site—IBET standing for Integrated Border Enforcement Team. (The first IBET was established in 1996 among law enforcement agencies in British Columbia and the state of Washington.)

The RCMP is capitalizing on partnerships already established through Windsor's IBET program to study radio interoperability.

"What we've done to date with the interim solutions," explains André Laflèche, "is implement devices that enable tactical interoperability. Agencies pick partners for predefined operations and use our devices to bridge their communications networks." At present, it's a somewhat cumbersome, labour-intensive process that requires connections to be established one by one. But Laflèche is less interested in the method of connectivity than in the way that connectivity is used.

"With the Windsor project, we want to see what agencies do with these communications tools—what their priorities are. The outcomes will inform our long-term interoperability strategy."

The approach was developed in collaboration with the expertise of both operational and technical personnel at the RCMP.

NEXT STEPS

Even as interoperability is being explored in the field, policy-related issues are being dealt with elsewhere. A draft agreement for shared communications, for example, has been developed by the RCMP and the IJI Secretariat, reviewed by the Windsor IBET and U.S. Customs and Border Patrol, and is undergoing legal review.

Looking ahead, André Laflèche and Francine Boucher agree that once a long-term strategy is developed, it may be time that a lead department such as Public Safety and Emergency Preparedness Canada (PSEPC) clarify the governance of radio interoperability as a national activity.

"We have a real sense that the will is there to make this happen," says Laflèche. "I think the work we're doing right now to define the requirements will help bring the various agencies' priorities into alignment and give us the direction we need to go forward."

*"WE'RE VERY
INTERESTED IN IMPROVING
RADIO INTEROPERABILITY, AND
WE RECOGNIZE THAT
SPECTRUM IS PART OF
THE EQUATION."*

INTEROPERABILITY
IN PROFILE

FOR THE

ASKING

THE RCMP'S INTEGRATED QUERY TOOL GIVES MEMBERS ACCESS TO MULTIPLE INFORMATION REPOSITORIES VIA A SINGLE INTERFACE

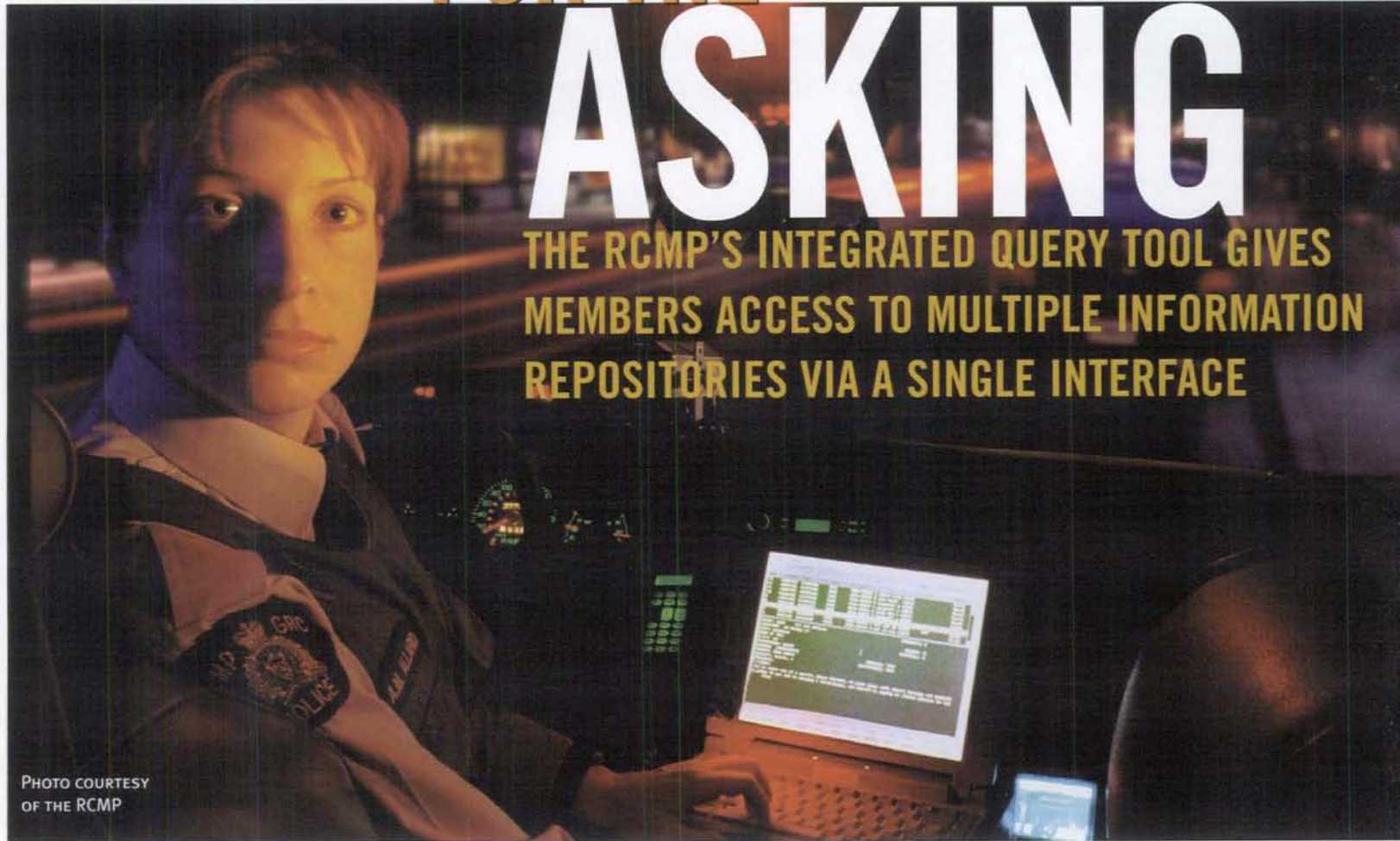


PHOTO COURTESY
OF THE RCMP

IN NOVEMBER 2001, THE RCMP BEGAN WORK ON A NEW ELECTRONIC CASE- AND RECORDS-MANAGEMENT SYSTEM, ONE THAT WOULD PROVIDE A WEALTH OF PRACTICAL FUNCTIONALITY AND BE TAILORED TO THE REAL-WORLD NEEDS OF FRONTLINE USERS. THAT SYSTEM WAS PROS: THE POLICE REPORTING AND OCCURRENCE SYSTEM.

THE VISION WAS FOR PROS TO REPLACE THE RCMP'S EXISTING RECORDS-MANAGEMENT SYSTEM, PIRS (POLICE INFORMATION RETRIEVAL SYSTEM). AND YET FROM THE OUTSET IT WAS CLEAR THAT THE REPLACEMENT PROCESS WOULD HAVE TO BE A GRADUAL ONE. THERE WAS TOO MUCH VALUABLE

INFORMATION STORED IN PIRS TO SIMPLY SHUT IT DOWN, AND, FOR A NUMBER OF PRACTICAL REASONS, THE MIGRATION OF ITS CONTENTS TO THE NEW SYSTEM WAS DEFERRED FOR FIVE YEARS.

FACED WITH THE PROSPECT OF MAINTAINING PARALLEL SYSTEMS—BOTH OF WHICH WOULD HAVE CONNECTIONS TO THE CANADIAN POLICE INFORMATION CENTRE (CPIC) DATABASE—THE RCMP DECIDED WHAT IT REALLY NEEDED WAS A TOOL THAT COULD INTERFACE WITH ALL THREE. AND SO THE INTEGRATED QUERY TOOL (IQT) WAS BORN.

INTEROPERABILITY IN PROFILE

ONE WINDOW, THREE VIEWS

As its name suggests, the IQT provides a single mechanism for querying the contents of PROS, PIRS and the CPIC core database—presenting results from all three in a standardized format. In the final stages of development, the IQT is slated for rollout alongside the official launch of PROS in summer 2004.

Users logging into the IQT—which is fully secured via an Entrust public-key infrastructure (PKI)—have a range of search options available: Person, Business/Organization, Property, Unique Identifiers, and Vehicles. Queries in any of these categories yield a result list based on the user's authorization privileges in the source systems. Members then have the option of viewing additional details and the related occurrence records from the result list.

An additional feature of the IQT is its ability to access the PIRS and PROS applications directly via a convenient single sign-on mechanism. Of course, to do so, members need the PROS application software available on their workstations—and must have the proper authorization to view the contents of each database. All source systems maintain their own authorization requirements.

THE IQT FACTOR

Kellie Paquette is the IQT Project Manager at the RCMP. She says IQT has been at once a challenging and exciting project. The development and supporting teams have worked hard to deal with a variety of technical issues, from working on a WebLogic platform to integrating with the Entrust PKI.

One of the RCMP's key aims was to incorporate CPSIN (Canada Public Safety Information Network) data standards into the IQT. This was a challenge from an interoperability perspective because PROS, having been built from an off-the-shelf solution, only partly conformed to the CPSIN standard, and PIRS, as a legacy mainframe pre-dating CPSIN, had no relation to it at all.

"The development of a data transformation component emerged to standardize query terms within the IQT," Paquette explains. "Of the 125 elements currently included in the IQT, I would say 90 percent are in accordance with the standard."

The IQT team's effort to conform to the CPSIN data standard was helped by the Public Safety and Emergency Preparedness Data Standards Secretariat (DSS).

"The DSS team has been very interested in our work all along," says Paquette, "because we're one of the first projects to work with the CPSIN standards—one of the first to apply them in a practical, real-world environment. Through our experience, the DSS has gained insights that have helped crystallize its content, and we on the IQT team have benefited by having the Secretariat actively help us achieve conformance."

"This is a solid solution," she concludes, "the solution does not require users to change their underlying systems. PIRS is still PIRS. CPIC is CPIC. Now there's PROS, and you can query all three using this one tool. I'm very excited to see how users respond to it."

Future plans for IQT include leveraging the investment in order to provide wider information-sharing capacity to the greater public safety community. The RCMP proposed that the National Criminal Justice Index (NCJI) initiative be replaced with an expanded initiative referred to as the National Integrated Interagency Information System (N-II). Work is currently under way to provide access to IQT to the Canada Border Services Agency.

Defining the terms: CPSIN DATA STANDARDS

"It's important to remember that what we're developing is an *exchange* standard, not a database standard," says Alistair Rondeau, Manager, Data Standards Secretariat (DSS). "In other words, we're not telling agencies how they should store information; we're giving them a framework and a vocabulary for *sharing* it."

In the last 18 months, work on that front has proceeded at a rapid pace. The final beta version of the CPSIN core data dictionary was completed in early spring; a gold release of the document is slated for Fall 2004.

"In defining each element of our data dictionary, we've worked from the best examples available," says Rondeau. "For example, the way we treat names is modelled on the approach of Citizenship and Immigration Canada, because that department has the most experience working with names that don't always follow the traditional North American formula of given name, middle name, family name."

To date, Rondeau says the DSS has received many compliments on the structure of its data dictionary from industry experts. Vendors have also followed its development closely, eager to ensure that their solutions meet the needs of government departments adopting the standard.


"It really is a new road we're on," Rondeau acknowledges. "And it's been great that project teams like IQT and SSDUE (Streamling Service Delivery Using e-Collaboration)—another RCMP information-sharing venture—are so keen to make the journey with us. I'm convinced that as people get to see the benefits of standardized information sharing—and the philosophy of information sharing that standards promote—we'll take a major step forward on the path to true justice information integration."

SPECIAL FEATURE ON BIOMETRICS:

A look at how this important innovation in security technology is transforming public safety and the fight against terrorism

Identifying the possibilities

BIOMETRICS IN CANADA



THE ONE THING THERE'S NO SHORTAGE OF WHEN IT COMES TO BIOMETRICS IS *OPINION*. EVERYONE SEEMS TO HAVE A THOUGHT ON THE SUBJECT—FROM THOSE WHO BELIEVE BIOMETRICS TO BE THE GREATEST-EVER ADVANCE IN SECURITY TECHNOLOGY TO THOSE WHO FEAR BIOMETRICS PRESENT A SERIOUS THREAT TO INDIVIDUAL PRIVACY.

THE TRUTH LIES AT NEITHER EXTREME. YES, BIOMETRIC TECHNOLOGY IS HIGHLY SOPHISTICATED. YES, PRIVACY HAS TO BE CONSIDERED WHEN DESIGNING BIOMETRIC SOLUTIONS. BUT THOSE SOLUTIONS DO NOT MAGICALLY ANSWER EVERY SECURITY NEED, NOR DO THEY INHERENTLY INTRUDE UPON THE BOUNDARIES OF PERSONAL INFORMATION.

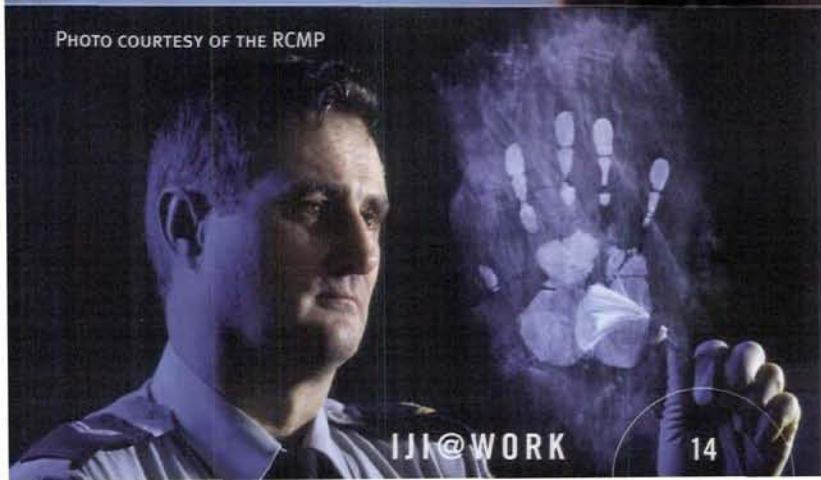


PHOTO COURTESY OF THE RCMP

SPECIAL FEATURE ON BIOMETRICS

Different biometric systems have different accuracy rates: while still subject to some debate, it is generally recognized that iris scans, for instance, are more accurate than facial-recognition solutions.

The challenge today—for agencies, organizations and governments that are responsible for security—is to determine the potential of biometric technologies, and to develop practical approaches to implementing them.

It is no small task, and there is much to consider. Biometric systems often employ proprietary software, for example. There can be a lack of interoperability between vendors' solutions. A case in point: one facial-recognition vendor's technology may not be able to share the image of a face with the system of another vendor due to the absence of interoperability standards. While many potential standards have been proposed for biometric technologies, only a very few have been ratified.

Accuracy is a further issue. Different biometric systems have different accuracy rates: while still subject to some debate, it is generally recognized that iris scans, for instance, are more accurate than facial-recognition solutions. And accuracy can vary by many factors, one of which is the level of control system operators have over the environments in which samples are taken. Collecting a fingerprint from someone voluntarily undergoing a criminal background check will yield a better-quality record than collecting the fingerprint of an uncooperative individual being charged with an offence. As a result, biometric systems cannot be fully automated; they must involve a verification process that depends on human intervention.

Finally, the implementation of biometric systems cannot be achieved without a complete analysis of privacy and legislative impacts. On this topic, it is necessary to proceed slowly and methodically to ensure that individual privacy rights are not compromised for the sake of a higher level of public safety and security.

This article looks at some of the biometric projects underway in Canada today from the perspective of the people leading them. Each feature illuminates a different piece of the biometric puzzle: from high-level policy-related issues to the nitty-gritty challenges of bringing a specific biometric solution to life.

BIOMETRICS DEFINING THE TERM

Electronic biometric systems are relatively recent phenomena, but biometrics themselves have been used by human beings for as long as there *have been* human beings. When you recognize someone you know upon seeing their face—in person or in a picture—you've essentially used a 'biometric' to identify that individual.

Biometric technologies—from fingerprint, ear and iris scanning to facial and hand-geometry recognition—replicate that process of identification (and authentication) electronically. (Authentication is the act of verifying that the person recognized is indeed who he or she claims to be.)

For *identification*, the scan of an individual biometric is compared to an archive of biometrics in a 'one-to-many' search. For *authentication*, the biometric accompanies some other form of identification, and is used to confirm that the identification is valid. This involves a 'one-to-one' comparison of records.

SPECIAL FEATURE
ON BIOMETRICS

Q&A

with Raj Nanavati on biometrics standards development

A PARTNER IN THE INTERNATIONAL BIOMETRIC GROUP (IBG), RAJ NANAVATI IS WIDELY REGARDED AS A LEADING AUTHORITY ON THE DEVELOPMENT OF BIOMETRIC STANDARDS. HE RECENTLY OFFERED HIS THOUGHTS TO IJI@WORK ON THE LAY OF THE LAND TODAY—AND WHERE THINGS MIGHT BE HEADING.

IJI@Work: How does the IBG see the present state of biometrics standards development?

Raj Nanavati: Undeniably, substantial progress has been made. But many of the more difficult areas to standardize—such as performance and accuracy—still have a long way to go before they could be considered even reasonably mature. The fact that biometrics is in most respects such a young discipline complicates standards development, because sometimes adopted standards enshrine inadequate technologies and approaches.

IJI@Work: Who's taking on the challenge?

RN: There are many organizations creating biometric standards, in fact. The International Labor Organization (ILO). The International Civil Aviation Organization (ICAO). The

National Institute of Standards in Technology (NIST). ISO/IEC (the International Standards Organization and the International Electrotechnical Commission). They're all looking at different biometrics: fingerprints, faces, irises.

IJI@Work: That raises another question, then: how will these standards be rationalized?

RN: Through the various liaison relationships maintained via ISO/IET JTC1 committees. Specifically, technical work being executed by ILO and ICAO is aligned with the proper committees within SC37 Biometrics, SC17 Cards and Personal Identification, and SC27 Information Technology Security Techniques. This is a time-consuming process, but these groups see the long-term value in aligning their formats and interfaces.



RAJ NANAVATI, PARTNER,
INTERNATIONAL BIOMETRIC GROUP

IJI@Work: What are your thoughts on biometrics in terms of accuracy rates and the impact of high-volume installations at airports and border crossings?

RN: It's a question that demands lengthy analysis, to be honest. To answer at a very high level: accuracy will be much less affected by the gritty details of algorithms and sensor specs than by things like integration into workflow, training, and end-user motivation. The volume of an installation does not have anything to do with accuracy rates—unless the application is an *identification* application.

SPECIAL FEATURE ON BIOMETRICS

From what we've seen so far in U.S. VISIT Status Indicator), fingerprint accuracy has been 'good enough' to meet the needs of inspectors. That's primarily because in addition to the biometric data, inspectors have been given access to more sources of data about visitors, especially via the Consular Consolidated Database. If CBP (the U.S. Customs and Border Patrol) is able to keep the average time for clearing false matches at or near the one-minute, seven-second mark discussed at the House hearing in January, the performance of the biometric itself is much less likely to become an issue. It still isn't clear, however, whether current throughputs can be maintained as the size of the US VISIT database increases, as the summer travel season arrives, and the installation of US VISIT at land ports is implemented.

IJI@Work: What are your thoughts on the efforts to create template standards for biometric information exchanges and interoperability? Doesn't a template standard take away from a vendor's proprietary competitive capabilities?

RN: Part of the question really is: will standard templates or images actually interfere with the ability of vendors to match a live biometric reading with an archived one? And there isn't sufficient data to know one way or the other. To be honest, not only has such testing not been executed, but there is no real agreement on how one would even test to measure such factors. In the AFIS (Automated Fingerprint Identification Systems) world, where interoperability image standards were developed, the technology has been able to function effectively. Template standards may be a different matter. In many cases, they heavily favour one vendor or approach.

IJI@Work: You mention AFIS. What's happening specifically with fingerprint biometric standards right now?

RN: There are at least two methods for comparing fingerprints: minutia-based matching and pattern-based matching. Minutia-based matching is often seen as better-suited to traditional applications where a large amount of fingerprint data is acquired. This is the case in the forensic AFIS market, for example. Minutia-based systems dominate there. Pattern algorithms are emerging more strongly for applications in which less fingerprint data is present. But the two types of matching are not interoperable. And the vendors of each type of solution tend to assert that their approach is more accurate.

Some within the industry have questioned whether pattern-matching solutions will ever be tested thoroughly enough to compare their true performance against minutiae-based solutions. Ultimately, the choice of which to use comes down to operational need. It's likely that pattern matching is 'good enough' if the performance focus of a solution is on throughput and 1:1 accuracy more than the 'needle in a haystack' production line work performed by an AFIS.

So, to get back to the question: image and template standards are being developed to allow for cross-system and cross-jurisdictional interoperability. There is considerable controversy in the area of pattern-matching standards, as the many different approaches cannot be reconciled through a single standard.

IJI@Work: This touches on the broader—and pressing—question of what's involved in picking a biometric that will be internationally acceptable?

RN: It is neither likely nor necessary that a single biometric must be 'picked' in order to maintain the integrity of international borders. In instances where a traveller is required to obtain a visa prior to presenting him- or herself at a border for inspection, the issuing country can choose whatever biometric it wants to secure the document. For visa-less travel—such as through the Visa Waiver Program—participating countries need only agree to exchange with one another the *means to decode and match* a traveller's biometric sample in the same format as that employed by the issuing country.

People have wondered about cultural barriers to the use of particular biometrics: is there a specific aversion among certain people to being fingerprinted, for example, or having their irises scanned? Based on the results of US VISIT to date, it appears that these objections are likely to be far less problematic than anticipated. Travelling to another country remains a privilege, not a right, and visitors have shown great patience and restraint so long as measures are considered reasonable. US VISIT has been relatively efficient. It applies to all visa holders and seems to be regarded as a reasonable security measure. I believe 'cultural barrier' issues will quickly become a non-issue if people perceive the border crossing experience to be efficient and fairly administered.

“It is neither likely nor necessary that a single biometric must be ‘picked’ in order to maintain the integrity of international borders.”

LOOKING AT THE **BIGGER PICTURE**

Canada's new National Security Policy gives prominence to biometric technologies

ALTHOUGH THE IDEA OF USING FACIAL, IRIS, OR FINGERPRINT SCANS WITHIN TRAVEL DOCUMENTS OR AT BORDER CROSSINGS USED TO BE SOMETHING RIGHT OUT OF THE MOVIES, IN LITTLE MORE THAN TWO YEARS BIOMETRIC TECHNOLOGIES HAVE PRACTICALLY BECOME THE GOLD STANDARD FOR CONFIRMING THE IDENTITIES OF TRAVELLERS AND OTHER PEOPLE ON THE MOVE.¹

At the end of April 2004, as part of its new National Security Policy, the Government of Canada announced it would begin issuing passports embedded with biometrically enabled smart chips by early 2005. It also announced that it would spend nearly \$100-million to enhance its capacity for electronic fingerprint screening. In fact, the new National Security Policy contains a Government commitment to work toward a

broader use of biometrics, having acknowledged that "the international community is increasingly using new technologies, including biometrics," to improve security.²

After 9/11, the federal government introduced voluntary biometric ID cards for travellers and iris scanning kiosks at major airports.³ At the same time, the government was pursuing a number of other biometric initiatives, including the Permanent Resident Card initiative and active cooperation with the International Civil Aviation Organization (ICAO) to develop globally interoperable security standards for facial recognition for travel documents.

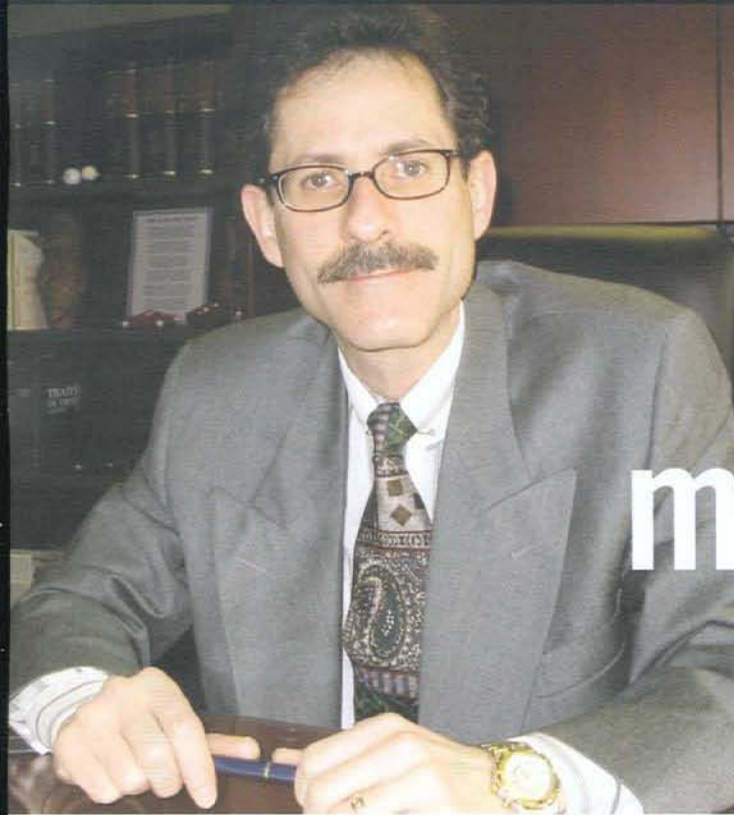
But when federal departments and agencies begin to consider using biometrics to enhance security, a number of critical questions need to be answered. For instance, what framework exists in Canada for implementing biometric solutions? When is a biometric

¹ Staples, Sarah. "Red-Hot Cybersecurity: Biometrics, shared databases create virtual borders," *Ottawa Citizen*, 6 May 2004, pp. G1, G3.

² *Securing an Open Society: Canada's National Security Policy* (April 2004), p. 45, www.pco-bcp.gc.ca

³ Staples, Sarah. "Red-Hot Cybersecurity: Biometrics, shared databases create virtual borders," *Ottawa Citizen*, 6 May 2004, p. G3.

PUT TO THE TEST:



Does facial recognition measure up?

Canada's Passport Office answers the question

JOCELYN FRANCOEUR, ADJUDICATOR AND
OMBUDSMAN FOR CANADA'S PASSPORT OFFICE

WHEN THE INTERNATIONAL CIVIL AVIATION ORGANIZATION (ICAO) CALLED FOR A BIOMETRIC TO BE INCLUDED WITH PASSPORT DOCUMENTS IN MAY 2003, IT SPECIFICALLY RECOMMENDED FACIAL RECOGNITION (FR).

"It makes sense," says Jocelyn Francœur, Adjudicator and Ombudsman for Canada's Passport Office. "After all, the passport already features an image of a person's face. It's no great leap to think about using FR technology to verify and link the bearer of a passport to an embedded picture in the book."

Yet questions have been raised about the accuracy and efficacy of FR technology, in the context of one-to-many verifications. In the United States, tests conducted through

the National Institute for Standards in Technology (NIST) have yielded less-than-superb results.

Canada's central agencies wanted to see for themselves if FR was up to the task. As the department with a readily available database of hundreds of thousands of images, the Passport Office volunteered to lead the study.

NO PRESUMPTIONS

"We hadn't made any decision to deploy FR," says Francœur, who directed the research project from an independent perspective. "Neither had any other agency. We were very open-minded about the testing; if FR failed, then it would fail. We had no stake in it."

Having secured funding to pilot-test FR

technologies and articulate the FR business case, the Passport Office set about developing a methodology that would yield practical, relevant results. That methodology (which was informed by existing models) involved comparing pairs of images: taking two different pictures of the same individual and determining if today's available technologies could make a match with a high degree of assurance.

"While other tests in the past have looked at 500 to 1,000 pairs of images," explains Francœur, "We used over 6,000 pairs. It's the largest number that's ever been employed for this kind of test. And we added 'noise' to make our test-case more like the real world. So there weren't just 6,000 pairs; there were

SPECIAL FEATURE ON BIOMETRICS

technology most appropriate for enhancing security? What are the next steps?

A team of Government of Canada engineers at the Communications Security Establishment (CSE) recently took steps to consider the answers to these types of questions. Between September 2003 and March 2004, the Government of Canada produced a pair of documents, based on surveys with nine federal government departments and agencies.⁴ The first document is the *Biometrics Business Requirements Report* and the second is a *Government of Canada Identification and Authentication Framework for Biometric Enabled Applications*. The business requirements and framework are designed to assist agencies to assess the viability of biometric options according to their needs.

A REALISTIC PERSPECTIVE

The reports do not document a broad spectrum of biometric business requirements, but focus instead on those that could be used in an actual, deployable system. CSE's mandate is to provide technical advice and guidance to the federal government on issues of security technology and technical solutions that can be adapted to the needs of individual departments.

The business requirements are defined in terms of purpose, environment, and integration issues: *What* are biometrics supposed to achieve? *Where* are they going to be deployed? How will they be incorporated into existing systems?

"Biometrics are just one of a number of possible authentication mechanisms in a secure system," explains Drew Smeaton, CSE Technical Manager for Biometrics. "The option has to match the security requirements of applications being used by an

agency or department and support a comprehensive approach to security."

The CSE team recognizes there is no one-size-fits-all approach, and that the particulars of any biometric solution are derived from an organization's specific functional requirements. "Biometrics don't exist in isolation and can't be approached in that manner," says Smeaton. This is where the value of the *Government of Canada Identification and Authentication Framework* document lies, putting parameters around the business requirements when it comes to developing solutions.

A FIRST STEP

The recently published Government of Canada documents are expected to be the first in a series. They describe the need to survey specific available technologies, define specific functional requirements, and explore policy-related issues as required next steps. "There are still a lot of policy questions around interfacing, sharing biometric information, and privacy," notes Smeaton.

As the government moves forward with biometric initiatives in the coming months, in accord with internationally recognized standards, a number of policy issues will no doubt need to be addressed. During that time, CSE's team of engineers intends to continue probing technical requirements for implementing biometrics within the Government of Canada. "We want to be able to provide a sound technical perspective for making decisions when the [policy] questions are raised."

10 BIOMETRIC BUSINESS REQUIREMENTS

The following Government of Canada business requirements for biometrics were identified:

1. A common need for the identification of unique individuals using non-sharable credentials
2. A common need for high-assurance authentication of those identified individuals
3. A cautionary approach to the introduction of biometrics (technology, privacy, user acceptance, etc.)
4. A determination of acceptable error rates and processing rates, depending on an application's environments
5. Consideration of industry-specific requirements for backwards compatibility with existing human characteristic systems
6. Consideration of project scope and scale (scalability varies between levels of government, with user bases ranging from hundreds to thousands to millions)
7. Integration of Biometric Identification and Authentication (I&A) services with a variety of application and physical access control deployment scenarios
8. Integration of I&A services with a variety of security model deployment scenarios, with particular consideration given to PKI interoperability
9. A testing and certification process to ensure biometric-enabled products are effective and meet recognized standards
10. Consideration of Government-wide policies and standards

Adapted from the Biometrics Business Requirements Report, 9 March 2004, CSE

⁴ Transport Canada, Canada Border Services Agency, the Privy Council, Correctional Service of Canada, the IJI Secretariat, the RCMP, the Canadian Air Transport Security Authority, the Department of Foreign Affairs and International Trade, and Citizenship and Immigration Canada.

Passport photos are particularly ideal for facial recognition, as they're taken under controlled conditions to a defined standard of quality.

also another 143,000 single images in the test database.”

The reason for engaging in such large-scale testing was a practical one. Canada's Passport Office processes more than 2,000,000 applications every year. Every one of the associated pictures would, in an FR environment, have to be queried against images of individuals included on security watch lists.

“Unlike including the picture on a chip—which would be inserted into a passport document and which would enable a one-to-one comparison—the biometric system we considered would be used in a one-to-many comparison mode,” observes Francœur.

HIGH CONFIDENCE

The Passport Office had its methodology scrutinized and validated successfully by the University of Ottawa's Department of Mathematics and Statistics. The size of the image sampling used provided a confidence level of 99.7 percent in the test results.

“The test results themselves have been quite positive, ranging from 75 percent to more than 90 percent depending on the quality of images and size of the gallery against which they were matched,” says Francœur. “Again, that's indicative of our approach. Each of the FR technology vendors that participated in our project had ten days to refine its processes, algorithms and the like. This is totally realistic. In a real-world implementation, no vendor would have just a few hours to prove a solution. There has to be a phase of tuning in to the specific challenge. And so what we've done is measure the best application of technology in the most strenuous circumstances we could simulate.”

The other reason for the high match rate, Francœur suggests, is that passport photos are particularly ideal for facial recognition, as they're taken under controlled conditions to a defined standard of quality.

“You do need good images,” he says. “The better the quality of pictures, the better your solution will perform.”

PRIVACY PROTECTED

Facial recognition, like other biometrics, involves the translation of an image—in this case, a human face—into a unique alphanumeric identifier called a template. (When people refer to the inclusion of a biometric “in the book”—the passport—they're referring to including the picture on a chip.) The template itself is not recorded on the passport, nor does the template contain any personal information.

“There's more personal information on your driver's license,” says Francœur, “than there is in a biometric template. In fact, the template is completely anonymous.”

For its test, the Passport Office applied the Privacy Commissioner's four criteria for determining the privacy implications of biometric technologies and other security measures, which are that:

1. the measure is demonstrably necessary to meet specific needs;
2. the measure is demonstrably likely to be effective in addressing the needs underlying the proposed deployment;
3. the loss of privacy is proportional to the security benefit; and
4. it can be demonstrated there is no less privacy-invasive measure that could achieve the same results.

Again, says Francœur, because photographs are already collected for passports today, and because the biometric template itself is anonymous, he and his team felt the technology satisfied all four requirements.

CONTINUED ON PAGE 44





SPECIAL FEATURE ON BIOMETRICS

THERE ARE MORE THAN A MILLION SEAFARERS AROUND THE WORLD TODAY—MEN AND WOMEN EMPLOYED IN THE MARITIME-TRANSPORTATION INDUSTRY. THAT INDUSTRY IS RESPONSIBLE FOR THE MOVEMENT OF MORE THAN 70 PERCENT OF THE WORLD'S COMMERCIAL GOODS; IN OTHER WORDS, IT IS ECONOMICALLY ESSENTIAL.

Since 1958, seafarers have had the option of procuring something called a Seafarers' Identity Document (SID). Issued by Member States of the International Labor Organization (ILO), this document was designed to facilitate seafarers' entry into ILO member countries for the purposes of leave, transit, transfer or repatriation.

In June 2003, responding to security concerns raised by the terrorist attacks of September 11, 2001, the ILO adopted a convention to amend the SID. The aim: to ensure that by increasing the security aspects of the document, the SID would continue to serve as a professional document while at the same time becoming an information-certification document. These changes will make the SID the world's first truly globally deployed biometric solution.

Donald Roussel, Director of Marine Personnel, Standards and Pilotage at Transport Canada, is this country's point man on the SID file. As such, he has a unique perspective on the process involved in defining such a large-scale solution.

Charting new waters

The Seafarers' Identity Document

Developing the world's first truly global biometric solution

CONSENSUS-BUILDING

"The first challenge for the ILO," reflects Roussel, "was to identify a biometric that could be implemented in any member country around the world, taking into consideration technological factors, economic disparities and issues of interoperability. That alone was an enormous task."

Out of these considerations, fingerprints were selected for the SID, as fingerprint technology is readily available, fairly straightforward, and relatively inexpensive.

The next requirement was to satisfy the concerns and expectations of a tripartite stakeholder group.

"Because the SID is the product of an international labour convention, workers, employers and governments have jointly contributed to defining how the new biometrically enabled document will work."

With the new SID, a seafarer's fingerprint is scanned and translated into a numeric sequence that is then printed, in bar-code format, onto the SID itself. On its own, that numeric sequence is entirely anonymous, and no information can be added to it once it has been printed.

"There is still a lot of mystery around biometrics these days," says Roussel. "Some people may be concerned that the information on the SID could be used to replicate an individual's fingerprint, but that's simply not the case. The biometric identifier in the barcode isn't a *representation* of a fingerprint, it's just a template or series of numbers. Others may be concerned that a person's privacy could be infringed upon. However, the manner by which the biometric is stored on the SID protects it from being altered or used without the card holder's consent."

STANDARDIZED FORMAT

The security model for the SID is similar in size and shape to that of a passport,

conforming to ICAO standards for such a document. Each SID is assigned a unique number by the issuing country. In addition to the barcoded biometric, it includes a digital photograph as well as basic information such as the name of the issuing authority, the full name of the bearer, and the date of the document's expiration.

In practice, the SID will be presented to port authorities or customs officials in ILO member countries. They will use special devices which will read the biometric information (the number in the barcode) and match it to the live fingerprint of the seafarer. They will then be able to verify the authenticity and validity of the SID either electronically or by contacting what's termed a 'focal point' in the issuing country. It is the responsibility of each country's issuing authority to provide 24-hour-a-day, seven-day-a-week verification services.

In Canada, Transport Canada will be the issuing authority of the new SID, just as today it issues the previous version. It plans to manage the entire process in-house.

"We have the facilities to produce the documents," says Roussel. "If we were to provide an SID to every seafarer in Canada, we would issue approximately 30,000 in total. This is a volume that Transport Canada can manage both securely and cost-effectively."

Roussel adds that his ambition is to see every Canadian seafarer receive one of the new SIDs—and ultimately for the document to become a required credential for the world's seafarers.

"It's a voluntary convention," he observes, "and always has been. While seafarers must carry a passport for transit, they are not currently required to also hold a SID. However, there are advantages to having both documents—for seafarers and border authorities alike. For seafarers, the SID accelerates the process of gaining access to ILO member

countries for shore leave and transit. For border authorities, it provides an extra measure of security and reassurance."

TOWARD THE HORIZON

The new SID convention (C-185) will come into force six months after the date on which the ratification of two members is registered with the Director General of the ILO. In other words, there's no fixed date. But Roussel anticipates it will happen within the next 12 months.

In that time, Canada still has some preparation to do. Formal authorization must be established for Transport Canada to issue the SIDs, and a national database of registered seafarers must be established. As well, the Canada Border Services Agency and Citizenship and Immigration Canada have to prepare themselves to process biometrically enabled SIDs possessed by international seafarers seeking to enter Canada.

Roussel is proud of the work that has been done on the SID to date, and confident that—as the first global biometric solution—it is going to achieve its objectives.

"There is a lot of technology out there related to biometrics, and a lot of standards. However, the SID convention is, to date, the only program to have received recognition from a large number of countries via an international organization. It is the world's first truly global biometric solution to enhancing marine security while meeting the needs of today's marine transportation industry in a global economy."

SPECIAL FEATURE
ON BIOMETRICS

IRIS RECOGNITION THE EYES HAVE IT

CANPASS Air simplifies border clearance for frequent flyers

WHILE MOST TRAVELLERS APPRECIATE THE NEED FOR STRINGENT SECURITY AT AIRPORTS, THOSE WHO FLY OFTEN MAY NOT—IF THEY'RE BEING HONEST—ALWAYS APPRECIATE HAVING TO GO THROUGH THE SCREENING PROCESS. AND ON THE OTHER SIDE OF THE COUNTER, MOST CUSTOMS AND IMMIGRATION OFFICERS WOULD AGREE THAT THEIR TIME IS BEST SPENT DEALING WITH UNKNOWN, POTENTIALLY HIGHER-RISK TRAVELLERS THAN WITH WELL-KNOWN, LOW-RISK ONES.

THESE TWO SETS OF CONSIDERATIONS ARE AT THE HEART OF THE CANPASS AIR PROGRAM. A JOINT INITIATIVE OF THE CANADA BORDER SERVICES AGENCY (CBSA) AND CITIZENSHIP AND IMMIGRATION CANADA (CIC), CANPASS AIR FACILITATES QUICK, SECURE ENTRY INTO CANADA FOR PRE-APPROVED, LOW-RISK AIR TRAVELLERS. THE KEY? AN IRIS BIOMETRIC THAT ACCURATELY AND INSTANTANEOUSLY CONFIRMS THE IDENTITY OF PROGRAM MEMBERS.

SEEING THE NEED

Aileen Dimasuay is the Senior Project Officer for CANPASS Air at CBSA. She explains that the choice of iris recognition technology was based on four criteria. Specifically, the chosen biometric had to:

1. Be **secure**—something that couldn't be lost or stolen.
2. Be usable via **technology available today**.
3. Be **accurate**.
4. Perform **rapid identifications** in a **non-invasive** manner.

Determining iris recognition technology to best meet all four, CANPASS Air opened its first enrolment centre at Vancouver International Airport in March 2003. Eight months later, a second enrolment centre was established at Halifax International Airport.

HOW IT WORKS

The CANPASS Air system records a photographic image of a traveller's irises. (Both eyes are used because each is unique—making the metric that much more secure.) This image is encrypted and stored in a secure database managed by CBSA. When a person registered in the program arrives in Canada after an international flight, he or she steps up to a self-serve kiosk equipped with a digital camera: the camera captures the member's iris and compares it with the one on file.

The traveller must answer some questions—onscreen at the kiosk. When the system verifies a member's identity, it prints a receipt, which the member presents to the officer upon exiting



the Customs Hall. For compliance verification purposes, travellers may also be pulled aside for a random inspection.

“What makes CANPASS Air so accurate and reliable is that the system will only accept the image of a live iris,” explains Dimasuay. “You can’t hold a picture up to the camera and trick it, for example. It looks for depth and certain critical dimensions, and it makes a comparison with the archived iris template that’s been recorded previously.”

For Dimasuay, part of what makes CANPASS interesting is the fact that, in many ways, it is a consumer-oriented biometric program.

“CANPASS Air is a voluntary program for frequent flyers,” she says. “It expedites the customs clearance process for them. At the same time, by taking ‘pre-approved’ travellers out of the line, CANPASS Air allows officers to focus on unknown travellers.”

Open to citizens and permanent residents of both Canada and the United States at present, eligibility for CANPASS Air membership may be extended to other visa-exempt countries and North American Free Trade Agreement business travellers

in the future. To date, some 3,000 people have registered.

In keeping with the consumer-oriented nature of the program, CANPASS Air has been promoted at airports and on airport websites, in travel publications such as *En Route* and *Bon Voyage* and via public announcements.

A THOROUGH REVIEW

The security strength of CANPASS Air is derived in part from its use of the iris biometric and in part from the thoroughness of its member-review process, which includes a formal application phase, a risk assessment whereby a search of five law enforcement databases is done, and a detailed, in-person interview at an Enrolment Centre—all before the biometric is recorded and a CANPASS Air card is issued. (That card includes personal identification information and a digital photograph.) The membership fee is \$50 per year.

GOING FORWARD

Later in 2004, the program will be expanded across the country with enrolment centres opening at:

- Lester B. Pearson International Airport, Toronto – June 2004
- Calgary International Airport – fall 2004
- Edmonton International Airport – fall 2004
- Winnipeg International Airport – fall 2004
- Montreal Trudeau International Airport – spring 2005
- Ottawa Macdonald-Cartier International Airport – spring 2005

“We’ve had great success so far,” says Dimasuay, “and we’re eager to build on it. But at the same time, we’re all aware the biometric is really a tool. It’s just one element of the larger security process.”

SPECIAL FEATURE
ON BIOMETRICS
PUTTING

the pieces together

MAKING REAL-TIME IDENTIFICATION A REALITY



SERGEANT C.H. CARL MCDIARMID, RCMP (LEFT) AND LLOYD BUNBURY, BUSINESS LEADER, RTID, RCMP WITH A LIVESCAN MACHINE.

THE REAL-TIME IDENTIFICATION (RTID) PROJECT BECAME PART OF THE CANADIAN GOVERNMENT'S CPSIN INITIATIVE IN 2000. ITS AIM IS TO STREAMLINE AND ACCELERATE THE RCMP'S INFORMATION AND IDENTIFICATION SERVICES, AND TO FACILITATE INFORMATION-SHARING INTERNATIONALLY—SPECIFICALLY WITH REGARD TO FINGERPRINT IDENTIFICATION, CRIMINALITY CHECKS AND MAINTENANCE OF THE NATIONAL CRIMINAL RECORD DATABASE.

TO DATE, MORE THAN THREE MILLION EXISTING FINGERPRINT RECORDS HAVE BEEN CONVERTED INTO A STANDARDIZED, HIGH-RESOLUTION ELECTRONIC FORMAT TO BE USED BY THE SYSTEM; MORE THAN 144 LIVESCAN BIOMETRIC READERS HAVE BEEN DEPLOYED ACROSS CANADA; AND A THOROUGH BUSINESS CASE HAS BEEN PRESENTED TO THE SENIOR EXECUTIVE OF THE RCMP.

The next step, according to Lloyd Bunbury, RTID Business Leader at the RCMP, is to bring all the pieces together.

"This is an enormous undertaking," says Bunbury. "But the end result is going to be well worth the effort. What we're talking about is shrinking the timeframe for identification and criminal records checks from weeks to literally just hours. And the advantages to Canada's law enforcement community will be invaluable."

The goals of RTID are: to return digitally submitted criminal identifications within two hours; to update all criminal records within 24 hours; and to process civil security clearances within 72 hours. The benefit of achieving such turnarounds is obvious when one looks at the present backlog of information requests—and the number of new records waiting to be entered into the existing file system.

"It would take over nine months to clear the backlog [of fingerprint and criminal-record transactions] if no new requests for updates were received," says Bunbury. "Without RTID, this backlog represents information the police may need today, and it can't be shared."

ALL IN THE PLANNING

The RTID business case outlines over 3,000 business and technical requirements for the system that will eventually replace AFIS (Automated Fingerprint Identification System), CREMMS (Criminal Records Entry Maintenance and Monitoring System), ADS (Active Document System) and the CNI (Criminal Name Index). Every one of those requirements has been reviewed by key stakeholders—including the system's ultimate end users and members of the vendor community that will have to build it.

SPECIAL FEATURE ON BIOMETRICS



"When you're dealing with a project of this scope," says Bunbury, "a national database that thousands of law enforcement and justice agencies will contribute to and extract information from, you have to be incredibly thorough in your preparations. By involving the vendors up front, we've been able to make sure that our requirements aren't unrealistic, unachievable, or skewed toward any one particular company's expertise."

A MULTI-MODAL BIOMETRIC SYSTEM

While fingerprints are at present the primary biometric identifier to be stored in RTID, the system in fact has the potential to handle a wider range of input, including palm prints and photographs for facial recognition.

Already, in a separate but connected project, the RCMP has implemented RAFIAS (Regional Authenticated Fingerprint ID Access System) at 90 sites across Canada, which provides police with the technology to record and upload crime-scene information electronically at 1,000 pixels per inch. This, too, will eventually be deposited in RTID.

"We'll be proceeding in phases," says Bunbury. "At first, only fingerprints will be searchable elements. But over time we'll be able to expand on the information available to include palms and faces."

With data coming from multiple sources—and to be shared with multiple agencies—standards are of tremendous importance to the RTID project team, particularly the National Police Services-NIST-Interface Control Document (NPS-NIST-ICD), which governs the sharing of biometric information.

"NPS-NIST-ICD is a variation of the ANSI-NIST (American National Standards Institute and National Institute of Standards and Technology) standard that was developed by law enforcement for law enforcement," says Bunbury. "It reflects the needs of the RCMP, the FBI, Interpol and other agencies. We know that ISO is working on its own biometric standards, and we've participated actively in its process because we want to be sure the work we've done to date is protected in the international environment. There's already been a significant investment of time and energy in consensus- and infrastructure-building."

THE WAY AHEAD

The deployment of LiveScan units in 2001-2002—and the creation of a networking interface—has allowed the RCMP to start processing urgent real-time identification requests electronically even while the development of the formal RTID system remains in progress.

"People have wondered why we implemented the LiveScans before we had a modernized database for them to feed into," Bunbury admits. "We felt it was good to put the tools in users' hands and build familiarity with them at the local level, so that they can be incorporated into their workflow processes. In the U.S., when authorities established a similar system to RTID, they built the infrastructure first and then had to wait while the users geared up. The practical reality is that, desirable as it might be, it's impossible to do both simultaneously."

Bunbury is therefore eager to deliver a request for proposals (RFP) to the technology vendor community and get the design and development phase of the project underway. He expects the RFP to be issued in the fall of 2004.

"The big challenge going forward," he says, "is dealing with the complexity of the system. In our 3,000 business requirements, we've been very careful to tell vendors *what* we need, but have avoided suggesting *how* those needs might be met. We need that to come from the experts; we want the benefit of their best practices."

Due to the complexity of the project, the RCMP has insisted on being a daily design partner in the process, working directly with developers to arrive at the final product.

"We really want to see this system developed for the sake of all law-enforcement agencies," says Bunbury. "It could be a key tool for ensuring public safety—especially as biometric data becomes increasingly important to police and public-safety work."

The deployment of LiveScan units in 2001-2002—and the creation of a networking interface—has allowed the RCMP to start processing urgent real-time identification requests electronically even while the development of the formal RTID system remains in progress.

PARTNERS IN PROFILE

A LOOK AT THE ONGOING
INFORMATION SHARING AND
COLLABORATION EFFORTS OF
PARTNERS IN THE CANADA
PUBLIC SAFETY NETWORK



JIM CHU, DEPUTY CHIEF CONSTABLE,
SUPPORT SERVICES DIVISION, VANCOUVER POLICE

LEIPs and bounds A “just do it” attitude yields rapid progress for IJI in Ontario and BC

IN FEBRUARY 2003, BRIAN COLLINS—THEN CHIEF OF THE LONDON POLICE SERVICE—SENT A LETTER TO HIS COLLEAGUES IN WINDSOR, TORONTO, OTTAWA AND ELSEWHERE IN ONTARIO OUTLINING HIS DESIRE TO DO SOMETHING ABOUT THE LACK OF INFORMATION SHARING AMONG POLICE IN THE PROVINCE. “TO MY MIND,” SAYS COLLINS, “IT WAS SCANDALOUS. I REALIZED HOW MUCH INFORMATION COULD BE SHARED—SHOULD BE SHARED, ROUTINELY—AND HOW EASY IT WOULD BE TO SHARE IT. MY LETTER SAID, ESSENTIALLY, THAT IT’S TIME WE DID SOMETHING ABOUT IT.”

AND SO THEY DID. IN A MEETING ON APRIL 16 OF LAST YEAR, REPRESENTATIVES OF VARIOUS ONTARIO POLICE SERVICES MET IN LONDON AND ESTABLISHED A VISION FOR INFORMATION SHARING. AN IMPLEMENTATION TEAM WAS STRUCK, RIGHT THEN AND THERE, WITH ELDON AMOROSO AND RICK GILLESPIE AT ITS HEAD. (AMOROSO IS THE SENIOR DIRECTOR OF THE INFORMATION TECHNOLOGY BRANCH OF THE LONDON POLICE; GILLESPIE IS SUPERINTENDENT OF THE FORCE’S CRIMINAL INVESTIGATION DIVISION.)

By September 17, 2003, London and Windsor were actively and electronically sharing information via a Law Enforcement Information Portal (LEIP). On November 6, Ottawa came online. And Toronto—the largest municipal police service in Canada—started contributing data as of March 31, 2004.

Pretty impressive for a little over a year's work—and just three formal meetings of the project team. And it's extremely gratifying for Collins, who retired in March 2004 after 34 years of service.

"Just in what's been done to date," says Collins, "I think we've effectively demonstrated that this kind of thing isn't a mystery—and doesn't have to be a bureaucratic nightmare. What it takes is commitment at the top, and one realistic goal at a time."

THE ADVANTAGE OF EXPERIENCE

It also helps to have the perspective of someone who's 'been there' before—who knows the potential pitfalls and how to avoid them. For the Ontario LEIP project team, that someone was Jim Chu, Deputy Chief Constable, Support Services Division, Vancouver Police. Chu is one of the driving forces behind British Columbia's own LEIP initiative, which has been up and running since September 2002. Today, all municipal agencies and RCMP detachments in BC have access to LEIP.

In BC, LEIP was necessitated by the development of PRIME: the Police Records Information Management Environment. The aim of PRIME was to outfit all BC police forces with a common, standardized records-management system (RMS)—a decidedly massive undertaking. In the interim, sharing

information between separate RMS installations is achieved through LEIP. When all police detachments in BC implement PRIME, LEIP will be the means by which they share information with external agencies.

"You learn a lot when you design, test and roll out our own application," says Chu. "Not just technically, but also in relation to project management and the logistics of implementation. I was more than happy to let the team in Ontario know what we'd discovered through our experience. When it comes to sharing justice information, there's absolutely no point reinventing the wheel."

Chu provided Ontario's LEIP team with the info-sharing Memorandum of Understanding (MOU) BC had developed, as well as results from research conducted into the implications of setting up an electronic system—legally and with regard to freedom-of-information issues. "We knew Ontario would have to adapt what we gave them to suit their provincial environment," says Chu, "but at least they had something to start from. We also helped them satisfy the security requirements for their architecture and network. We'd had a lot of conversations with security officials at the RCMP and we'd cleared a lot of hurdles. That experience benefited the Ontario group."



"YOU LEARN A LOT
WHEN YOU DESIGN, TEST AND ROLL
OUT OUR OWN APPLICATION. NOT JUST
TECHNICALLY, BUT ALSO IN
RELATION TO PROJECT MANAGEMENT
AND THE LOGISTICS OF
IMPLEMENTATION."

SHOW, DON'T TELL

Chu explains that virtually from the outset, the BC team knew that the best way to secure widespread 'buy-in' for LEIP was to build the system—on whatever scale might be possible—and prove its advantages in action. So the project team recruited police forces to link up to LEIP without obligating them to contribute anything.

To implement a project in that way, notes Chu, you have to be extremely cost-effective. "We didn't hire any high-priced consultants," he says. "We had police agencies contributing their own staff to our project—hundreds to thousands of human-resources hours. That's how you have to do it. And we had support from the Integrated Justice Information Secretariat, for which we are very appreciative."

Once the value of the system became clear, of course, users grew increasingly eager to give something back, Chu explains.

"People got online and saw what they could get out of the system—they wanted to contribute. And once high-level decision makers saw how well LEIP performed, they recognized it was the right thing to support; they resolved to keep it going."

"We had police agencies contributing their own staff to our project—hundreds to thousands of human-resources hours. That's how you have to do it."

HOW LEIP WORKS

In Ontario, police services on the LEIP system continue to upload occurrence information into their individual records management systems. Basic information such as persons and vehicles can be searched, via LEIP, by any member of any force connected to the system. That search yields an index-style report of top-level information. Members can then drill down, as authorized, into the appropriate RMS to get more detailed information.

PICTURED (FROM LEFT TO RIGHT):
CHIEF BRIAN COLLINS (RETIRED), SENIOR DIRECTOR ELDON AMOROSO,
SENIOR BUSINESS ANALYST CASE HUYSMANS, AND
SUPERINTENDENT RICHARD GILLESPIE

PHOTO COURTESY OF LONDON POLICE SERVICE



OPENING UP

In Ontario, unlike BC, there has been no province-wide move to institute a common RMS. Consequently, the Ontario LEIP system had to be designed openly, ensuring that any RMS could connect.

"Already, we've shown that we can accommodate a variety of systems," says Senior Director Eldon Amoroso. "London, Windsor and Ottawa all use the same brand of RMS, but Toronto has a homegrown system, and we successfully started loading their production data in March."

Having demonstrated its interoperability, Amoroso says there's no reason why Ontario's municipal LEIP system couldn't interface with a whole range of other systems—from the shared RMS of the OPTIC group (40 municipal police agencies and the Ontario Provincial Police) to the BC LEIP itself.

Because multiple RMSs are involved in the Ontario system, establishing a data standard

for the interface was key. What one system classifies as a 'subject', for example, another might classify as a 'suspect.'

"We had a business analyst sit down with all the departments involved to look at those issues and develop a working standard for the LEIP system," says Amoroso. "Everybody continues to input data into their own RMS in their own way, but when they're querying LEIP or reviewing search results, there's a standard terminology that's used."

Amoroso says the LEIP data standard is very close to the CPSIN data standard, and that marrying the two precisely will not be an onerous task in the future.

EARLY RESULTS

Detective Superintendent Rick Gillespie says that Ontario LEIP users have already seen the system's real-world advantages. He cites the example of a domestic-violence

case. There was no record in London that a subject accused of domestic violence had been charged previously with a similar offence in Windsor. But a LEIP search by the investigating officer revealed that more complete history—providing additional information for the "Show Cause" portion of the requisite bail hearing. Without LEIP, that crucial bit of history might have been missed.

"It also shows you how important LEIP is for breaking down information silos," says Gillespie. "Windsor is right down the road from London, and yet that information wouldn't otherwise have been shared."

In British Columbia, Jim Chu says the experience has been similar. "You look at Boundary Road in Vancouver," he points out. "On one side of the street you have Vancouver PD patrolling; on the other, it's the RCMP. Crooks benefit from the inability of police agencies to share information."

“WE MADE SURE FROM THE
START THAT WHEN THE TEAM SAT
DOWN TO TALK, WE WEREN'T THERE TO
DISCUSS PROBLEMS, WE WERE THERE
TO MAKE DECISIONS ABOUT HOW
TO GET THINGS DONE.”

TAKING IT FURTHER

Eldon Amoroso says that he and his Ontario LEIP colleagues have received numerous requests from other police services in the province to join up. “It’s really gathering momentum now, which is exactly what we’re looking for. Honestly, with the technology we have today, we could connect the entire province of Ontario within the next year.”

While Ontario continues to add members to its LEIP network, BC is pioneering still other new directions.

“Right now in Victoria,” says Jim Chu, “we’re extending LEIP information to field officers wirelessly. So members out on the

And, as was mentioned previously, BC LEIP serves as a bridge to the province’s standardized PRIME RMS. Work is underway to migrate PRIME from a network of discrete databases into one single, massive, virtual database. Why, one might wonder, when LEIP is already giving departments access to each others’ RMSs?

“More access,” says Chu, plainly. “It’s all about getting more information faster. LEIP gives access to about 90 percent of the information in departmental RMSs. It handles common queries. But it can’t do everything. With a single multi-jurisdictional RMS, it’s all there. But that kind of RMS is still some time away from being a reality—and we needed something yesterday.”

To date, the Victoria capital region—which consists of four municipal police departments—is already on the new multi-jurisdictional PRIME system, including the full LEIP interface. Vancouver and BC’s other lower-mainland police departments are slated to migrate later this spring from their stand-alone databases to the multi-jurisdictional PRIME as well.

And, as was mentioned previously, BC LEIP serves as a bridge to the province’s standardized PRIME RMS. Work is underway to migrate PRIME from a network of discrete databases into one single, massive, virtual database. Why, one might wonder, when LEIP is already giving departments access to each others’ RMSs?

“More access,” says Chu, plainly. “It’s all about getting more information faster. LEIP gives access to about 90 percent of the information in departmental RMSs. It handles common queries. But it can’t do everything. With a single multi-jurisdictional RMS, it’s all there. But that kind of RMS is still some time away from being a reality—and we needed something yesterday.”

REFLECTING ON SUCCESS

Brian Collins, Eldon Amoroso and Rick Gillespie all recognize that a variety of factors have contributed to the initial success of the Ontario LEIP project. Commissioner Zaccardelli of the RCMP was committed to supporting it—and the RCMP provided the connectivity infrastructure via its NPS network. That accelerated implementation. And

start-up costs were partly covered by two PACTAD grants from Statistics Canada.

But by far the most important determinant was the will to get something done.

“We set up a server, we established connections, we started growing from there,” says Collins. “We made sure from the start that when the team sat down to talk, we weren’t there to discuss problems, we were there to make decisions about how to get things done. We knew it wouldn’t be perfect from the get-go; we knew we weren’t going to build the whole system in one shot. But in this era of globalized crime, we were committed to doing *something*. LEIP is really part of our bigger philosophical picture, a growing recognition that integrated policing is absolutely essential to public safety in the 21st century.”



PHOTO COURTESY OF VANCOUVER POLICE

street can see real-time information coming from Vancouver. And Vancouver PD has started sharing information with the Richmond RCMP detachment. That’s huge for us. I don’t know anywhere else in Canada where a non-PIRS agency⁵ can access RCMP information on their laptops in the field.”

⁵ PIRS is the RCMP’s legacy RMS. While a new system, PROS, is being rolled out in many parts of the country, Richmond and other BC-based RCMP operations are remaining, for the time being, PIRS users.

**Commitment from
the top**

The following police chiefs committed their organizations to supporting phase one of Ontario LEIP:

- Chief Brian Collins, London Police Service
- Chief Glen Stannard, Windsor Police Service
- Chief Vince Bevan, Ottawa Police Service
- Chief Julian Fantino, Toronto Police Service

LEIP is really part of our bigger philosophical picture, a growing recognition that integrated policing is absolutely essential to public safety in the 21st century.

Connecting partners in

Quebec and Saskatchewan

CORRECTIONAL SERVICE CANADA'S OFFENDER MANAGEMENT SYSTEM

AMONG CANADA'S CRIMINAL JUSTICE PARTNERS, EFFORTS TO RENEW CASE-MANAGEMENT SYSTEMS ARE FOCUSED ON MORE THAN JUST DEVELOPING NEW WAYS TO SERVE THEIR EXISTING CLIENT BASE—IMPROVED CONNECTIVITY AMONG EXTERNAL COUNTERPARTS IS JUST AS IMPORTANT. IN THIS RESPECT, CONSIDER THE ACHIEVEMENTS OF CORRECTIONAL SERVICE CANADA'S OFFENDER MANAGEMENT SYSTEM (OMS) RENEWAL TEAM. SINCE EARLY 2001, THIS TEAM HAS MADE IMPORTANT STRIDES TO ENHANCE THE OMS, WHICH GATHERS, STORES AND RETRIEVES INFORMATION ON OFFENDERS IN CANADA'S FEDERAL CORRECTIONAL SYSTEM.

"Information sharing has been a key priority for the OMS Renewal Project since the beginning," explains George Pinatel (Manager, Information Sharing, and Communications, OMS Renewal Project). "That's something we're particularly proud of, since we are the only organization within the Canada Public Safety Information Network that has thus far achieved a level of information exchange with outside organizations."

By 2005, over 2,000 new external users will have been connected to the renewed system, providing data exchanges that are controlled, secure and limited, according to access permitted by law. While police services across Canada have benefited from OMS access since 2003 (profiled in *IJI@Work* Issue #3), connectivity has also been granted to provincial and territorial-level corrections agencies in Canada's correctional system. Agreements with Quebec and Saskatchewan were among the first to be reached (a separate service agreement has also been

reached with the Yukon Territory, but it differs in scope and application).

Thanks to individual Memoranda of Understanding reached with the two provinces, correctional authorities in these jurisdictions are now benefiting from improved connectivity with the Correctional Service Canada (CSC). Through these agreements, the provinces have round-the-clock access to a special OMS interface menu, designed specifically for their needs by the OMS Renewal Team.

With respect to the agreements reached with Quebec and Saskatchewan, the result has been an all-new electronic exchange of information that provides a more fulsome array of facts on offenders in their care.

"These agreements give our counterparts access in read-only mode to OMS files on particular offenders on a need-to-know basis," explains Pinatel. "That basis is determined when they have an individual in their custody who was formerly an offender in the

PARTNERS IN PROFILE

federal system.” It also provides for a reciprocity arrangement, in which CSC is given access to the provincial and territorial offender management system for offenders held in their custody in the past.

The controls on information exchange are essential to adhere to privacy legislation and to the *Corrections and Conditional Release Act*. Still, the level of connectivity provided through these agreements is vital to public safety. Decisions in the correctional system can have a direct impact on the safety of citizens. Every additional bit of information on an offender that can be exchanged and added to a case file *can* make a difference. For example, Pinatel cites the findings of a 2002 Quebec inquiry into the death of a 13 year-old boy who was murdered in 2000 by an offender who had been released on parole by provincial corrections authorities. The inquest recommendations included a call for improved information sharing between the Quebec Parole Board (la Commission québécoise des libérations conditionnelles) and their federal counterparts. In doing so, provincial authorities will be able to immediately determine whether an offender whose file they are reviewing has previously served time in a federal corrections facility for a federal offence. Thanks to the reciprocity arrangement, the same connectivity is given to federal authorities regarding provincial information.

Implementation of OMS connectivity with Quebec and Saskatchewan (as well as the separate agreement with the Yukon Territory) was just the start to the information-exchange activities undertaken by the OMS Renewal Team. Additional agreements have since been negotiated with British Columbia, New Brunswick, as well as with Newfoundland and Labrador. The implementation phase of each of these agreements will conclude before the end of 2004.

The OMS Renewal Team is also focusing on the next stage of its project, Pinatel explains. “Once we’ve finished our work on OMS migration,” he says, “we will start looking at ways to transfer offender information from system to system among federal, provincial and territorial partners in Canada’s correctional system to eliminate duplication between jurisdictions.” That undertaking is expected to be completed within the next two years.



PHOTO COURTESY OF
CORRECTIONAL SERVICE CANADA

PARTNERS IN PROFILE

Quebec and Saskatchewan

perspectives on OMS connectivity

TO OBTAIN A PERSPECTIVE FROM QUEBEC AND SASKATCHEWAN—THE TWO PROVINCES THAT HAVE FULLY IMPLEMENTED OMS CONNECTIVITY—IJI@WORK SPOKE WITH PROVINCIAL OFFICIALS RESPONSIBLE FOR THE MANAGEMENT AND ADMINISTRATION OF THESE PROJECTS WITHIN THEIR RESPECTIVE DOMAINS: PIERRE BÉRUBÉ (SYSTEMS ANALYST, CORRECTIONAL SERVICES QUEBEC, MINISTRY OF PUBLIC SECURITY), AND GEORGE CLARK (INFORMATION SYSTEMS MANAGER, SASKATCHEWAN CORRECTIONS AND PUBLIC SAFETY—ADULT CORRECTIONS DIVISION).

IJI@Work: What were the key challenges you encountered in implementing OMS connectivity, stemming from the Memorandum of Understanding reached with Correctional Service Canada?

Bérubé (Quebec): For us, a key challenge was to develop all the necessary information-exchange protocols within our organization. To meet the requirements of the Memorandum of Understanding, we had to implement common business practices to comply with security requirements at Correctional Service Canada. Once this step was addressed, we were able to get to work on the technical component, involving testing of our systems to ensure compliance and secure connectivity.

Clark (Saskatchewan): One of our primary tasks was to identify the conditions under which information may be shared. Once that was achieved, we had to define a way for staff to request the information and establish structures to distribute and store the information.

IJI@Work: In practical terms, how does your province benefit from this agreement on information exchange?

Bérubé (Quebec): The work that was required to meet the requirements of the Memorandum

of Understanding with CSC was challenging. It wasn't easy—it took us approximately six months to complete this task—but in our view it was a good thing that this step was required. It compelled us to look carefully at our business practices and at the steps involved in exchanging information within our offender case-file system. Bear in mind that it's difficult to be specific about the benefits of information exchange, due to the nature of the correctional system. While improved information sharing derived from our agreement is something that we are now using every day, the benefits ought to be transparent. They should blend seamlessly into the existing systems that we already had in place in the Quebec correctional system. In a manner of speaking, when it comes to information sharing about offenders, no news is good news.

Clark (Saskatchewan): This project coincided with a major case-management policy thrust for adult corrections in Saskatchewan. Our approach consisted of developing one case

plan for each offender, and sharing the details of that plan with appropriate case managers. This resulted in the implementation of online risk assessments, correctional plans and progress reports including special updates about an offender's participation in programs such as the Offender Substance Abuse Prevention Program. The ability to review the experience of offenders with our federal counterparts improved the decision making both around risk-needs assessment and intervention strategies appropriate to the case.

IJI@Work: Are you pleased with the outcome of the memorandum of understanding?

Bérubé (Quebec): Yes. For us, it was a very encouraging project. It demonstrated that we can work together to address concerns that matter to our citizens, such as public safety. We're especially pleased with the learning opportunity that this exercise afforded: we're a smarter organization thanks to this experience.

Clark (Saskatchewan): The memorandum is important for us. It provides a basis and the broad parameters under which information is shared. As the project was rolled out, we had to make sure that the Memorandum of Understanding and all relevant legislation was adequately explained to our users. This discussion continues to evolve as staff change and new situations are identified where individuals feel that a training refresher is needed.



MICHAEL BOUDREAU, DIRECTOR, PROGRAMS AND PLANNING, COMMUNITY AND CORRECTIONAL SERVICES, DEPARTMENT OF PUBLIC SAFETY, NEW BRUNSWICK AND ROBERT CYR, PIMITS PROGRAM DIRECTOR, DEPARTMENT OF PUBLIC SAFETY, NEW BRUNSWICK

GETTING IT DONE

New Brunswick is making strides in the realm of IJI

THERE ARE SEVERAL ESSENTIAL INGREDIENTS FOR THE SUCCESS OF INTEGRATED JUSTICE INFORMATION (IJI). TECHNOLOGY, OBVIOUSLY, IS ONE: HAVING THE RIGHT TOOLS TO MEET BUSINESS REQUIREMENTS. POLICY IS ANOTHER: BUILDING THE FRAMEWORKS WITHIN WHICH INFORMATION CAN BE SHARED EFFECTIVELY.

PROJECT MANAGEMENT IS A THIRD. AND IT'S A DIRECT RESULT OF SKILLFUL PROJECT MANAGEMENT THAT CRIMINAL JUSTICE AGENCIES IN NEW BRUNSWICK HAVE MANAGED TO MOVE FORWARD WITH TWO KEY INFORMATION-SHARING INITIATIVES IN RECENT YEARS: A POLICE INFORMATION MANAGEMENT/INFORMATION TECHNOLOGY SHARING PROJECT KNOWN AS PIMITS; AND A CLIENT INFORMATION SYSTEM (CIS) FOR THE PROVINCE'S DEPARTMENT OF COMMUNITY AND CORRECTIONAL SERVICES.



HARD-WON WISDOM

Michael Boudreau is the Director of Programs and Planning, Community and Correctional Services, Department of Public Safety in New Brunswick—and the operational CIS project leader. He says that the province's interest in integrating justice information systems goes back to the early 1990s.

"There was a massive project undertaken at that time called NBIJ—New Brunswick Integrated Justice." Boudreau says it was extremely ambitious: a top-down, comprehensive project to connect justice systems in the province electronically. "In the end, it proved impossible to realize. It was too big, too expensive, and it failed. But out of

that experience we learned some invaluable lessons. Most importantly, that with these kinds of projects you can't expect to achieve all your goals at once."

Another key realization was that no matter how important the technological component may be, IJI projects can't be solely IT-led. For a system to succeed, it needs to meet the on-the-ground business requirements of users.

"We took some of our best people off the floor, so to speak, and involved them in the design and development process," says Boudreau. "For sure, there's a cost associated with that kind of decision—a human-resources cost. But we certainly wouldn't do it any differently."

PARTNERS IN PROFILE

THE RIGHT SOLUTION

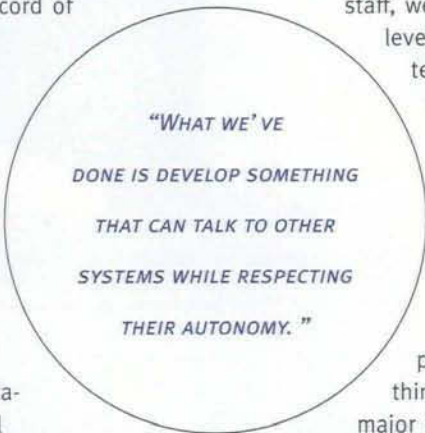
The CIS was launched in 1999 and completed in 2002. Installed at 70 sites across New Brunswick, it encompasses the dispositional phase of the judicial process—the phase in which sentences are calculated and carried out. Fully secure, the CIS contains information on both adult and youth offenders in institutions and community-based correctional environments. It also keeps a record of victim information.

The CIS was designed to interface with the province's Department of Justice and Department of Family and Community Services systems, as well as with the federal government's Offender Management System (OMS). (In fact, the CIS team had an IT representative from the Correctional Service of Canada to help ensure that the CIS system would interface with the federal OMS.)

Developed in accordance with federal data standards, the CIS is currently being outfitted to share information with the Canadian Centre for Justice Statistics (CCJS).

Accessed via a secure web browser, the CIS is a completely integrated system with capabilities that include the provision of real-time offender information, a complete case-management module and—a feature that has generated significant interest among other correctional services organizations—an automated sentence calculator.

"What we've done," explains Boudreau, "is develop something that can talk to other systems while respecting their autonomy. We know from past experience that trying to build everything from the ground up is just too complicated. So we developed the system we needed, and a mechanism for interfacing with others."



WARMLY RECEIVED

Boudreau says there was great enthusiasm for an electronic system like CIS within Community and Correctional Services—despite the fact that very few front-line employees of the department had previous computer experience.

"Until CIS, we had been entirely paper-based," says Boudreau. "When we surveyed staff, we found there wasn't a high level of comfort or aptitude with technology. But virtually everyone recognized that we could make our systems better."

To facilitate adoption of the CIS, the department provided extensive technology training in everything from basic keyboarding skills to full-fledged computing boot camps. "I really think this has been another major key to our success," says

Boudreau. "People appreciate that we took time to help them reach a place of comfort with the new system. It showed in their eagerness to learn. Overwhelmingly, people wanted the training."

MEASURES OF SUCCESS

The New Brunswick CIS has received no small share of attention from other criminal-justice organizations in Canada. Its data-encryption model is being promoted by Public Safety and Emergency Preparedness Canada's IJI Secretariat as the foundation for a national standard. Correctional Service Canada has surveyed some 120 similar systems around the world and ranked the CIS among the top three. And in 2002 it received both a Canadian Information Productivity Award and a Knowledge Industry Recognition Award—as well as a special acknowledgment from the Premier of the province.

"We're very proud of all our achievements," says Boudreau. "They're the result of a lot

of hard work. The important thing is to take one step at a time. As much as a shared nationwide system may be desirable, it's not going to happen in the immediate future. But there's lots you can do if you have the will and the commitment. And with small, incremental steps, people see the benefits quickly, and that inspires them to join in."

ALL FOR ONE

The vision of PIMITS is to electronically connect all police forces throughout New Brunswick—enhancing their capacity to develop and share intelligence in ways that reduce the threats of organized crime, serious crime and terrorism. It's part of the strategic plan of the province's Department of Public Safety, and its genesis goes back at least as far as that of the CIS.

Robert Cyr is PIMITS Program Director at the New Brunswick Department of Public Safety. He says the lessons learned developing the CIS have been extremely helpful in propelling PIMITS forward. "We're doing this project in a very lean, very focused way," he says. "Our program office is made up of two people—including me. We're drawing on the technical expertise of municipal police forces and the New Brunswick Department of Public Safety. As was done with CIS, we're taking an incremental approach, setting realistic milestones and working toward them."

That approach was clearly defined by the PIMITS Steering Committee, on which sit senior members of every police force in New Brunswick. Cyr cites as an example the establishment of a technological infrastructure that will support PIMITS information-sharing. A private, secure, closed-loop network, this infrastructure has already benefited agencies even while other elements of the system are still under development.

"Before we built the infrastructure, some police forces had to gather motor vehicle information from the provincial mainframe via a low-bandwidth dial-up connection,"

says Cyr. "It was time-consuming and awkward. Now they can use the PIMITS infrastructure and gain direct, high-bandwidth access."

Because the PIMITS infrastructure is private and secure, it has the potential to fulfil the security requirements of the CPIC renewal team. By way of background: two types of connection to CPIC are possible—one via CPIC for Windows, and the other via what's known as a message-oriented middleware (MOM) interface. CPIC for Windows applies to standalone PCs; the MOM interface model applies to networked PCs, for which security is a key concern. If PIMITS were able to establish an interface with CPIC, the advantages would be great for law enforcement agencies throughout New Brunswick—because the interface would be shared by all of them. This would be enormously helpful for smaller detachments, as it would otherwise be prohibitively expensive for them to acquire the MOM-interface technology to connect to CPIC independently.

Now that the network infrastructure has been built, the next step laid out by the multidisciplinary Steering Committee is to establish an information-sharing "clearinghouse."

MAINTAINING AUTONOMY, SHARING INFORMATION

The PIMITS clearinghouse might be better understood as a portal. It will allow local records-management systems (RMS) to connect to the shared PIMITS infrastructure, while giving individual police organizations the freedom to maintain their own databases.

This is important from a usability perspective, as it means front-line officers gain the benefit of new functionality without having to learn their way around a brand-new and unfamiliar system.

To achieve this functional transparency, it is a design objective of PIMITS to translate native RMS data to the CPSIN data standard via a 'black-box' solution. Through the clearinghouse, members will be able to conduct searches and queries beyond boundaries of their local RMS.

To govern PIMITS information sharing, the PIMITS project team is developing a Memorandum of Understanding in collaboration with the IJI Secretariat. This MOU, when finalized, will capture the vision of PIMITS and articulate the mechanics of how information will be shared.

EYE ON THE FUTURE

While it's taking an incremental approach, the PIMITS project team's view is decidedly long term. "You have to keep the future in mind, even while you focus on what you can and need to get done right now," says Cyr. "For example, we've had lots of conversations with the CPIC renewal team; we know we're going to want to link to that system, that our interface should interoperate with that system. That's why we built the architecture we did—one that's secure and that will meet our bandwidth requirements down the road."

As with any IJI project, the long-term view begs certain financial questions, such as

"where's the budget going to come from to support the system over time?"

The answer in the case of both the CIS and PIMITS is public-private partnerships, at least in part. Working closely with private-sector technology partners, the CIS and PIMITS teams hope to commodify the systems they're building.

"Other jurisdictions face the same challenges we do," says Michael Boudreau. "They're going to need solutions. We've made an arrangement whereby our CIS IT partner, xwave, can go re-market the intellectual property they've developed for our system in other jurisdictions. And we'll get a royalty from any sales, which would provide us with a stream of funding."

To date, all of Canada's provinces have looked at the CIS; so has the State of Virginia and the State of Maine—where a purchase has been made. It's even been demonstrated as far afield as Singapore.

This enterprising model is just another in a long list of innovations New Brunswick's IJI community has made—innovations that Michael Boudreau and Robert Cyr believe will apply elsewhere.

"We talk about New Brunswick as a microcosm," says Boudreau. "It's a great place to learn lessons that may be applicable at other levels. And we're absolutely ready and willing to share what we know."

The vision of PIMITS is to electronically connect all police forces throughout New Brunswick—enhancing their capacity to develop and share intelligence in ways that reduce the threats of organized crime, serious crime and terrorism.

Information sharing:

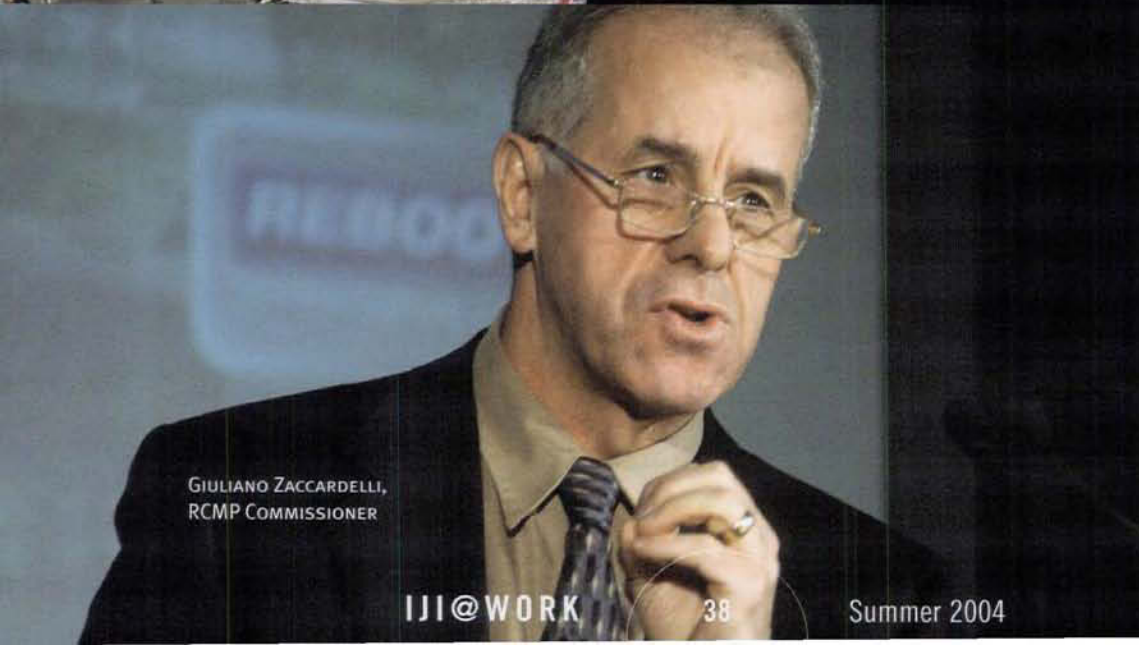


CHIEF VINCE BEVAN,
OTTAWA POLICE SERVICE

**Highlights from the
Canadian Association
of Chiefs of Police
forum on information
sharing and
interoperability**



CHIEF EDGAR MACLEOD,
PRESIDENT, CACP



GIULIANO ZACCARDELLI,
RCMP COMMISSIONER

MAKING IT HAPPEN

"KICK-START YOUR THINKING FROM CAN'T DO IT, TO JUST DO IT." THAT WAS A KEY MESSAGE TO EMERGE AT A NATIONAL CONFERENCE ON INFORMATION SHARING AND INTEROPERABILITY, ORGANIZED BY THE CANADIAN ASSOCIATION OF CHIEFS OF POLICE (CACP), HELD NOVEMBER 24-26, 2003, IN MONTREAL, QUEBEC. THIS THREE-DAY GATHERING, ENTITLED *POLICE AND ENFORCEMENT PARTNERSHIPS: MAKING INFORMATION-SHARING HAPPEN*, WAS DESIGNED TO SERVE AS A SPRINGBOARD FOR CHIEFS AND HEADS OF LAW ENFORCEMENT TO TAKE IMMEDIATE STEPS TO IMPROVE INTEROPERABILITY AND INFORMATION-SHARING CAPABILITIES AMONG CANADA'S CRIMINAL JUSTICE PARTNERS.

This forum was well attended—comprised of 160 senior-level delegates representing police, governments and law-enforcement agencies across Canada. Participants heard a thoughtful keynote speech by renowned jurist, Justice Archie Campbell, who shared his perspective on information sharing, based on his widely quoted 1996 report on the Paul Bernardo investigation. Citing criminal cases where information sharing was a hindrance to the efforts of police, he contended that a fundamental shift in attitude is necessary among police and law-enforcement agencies. "If people don't want to share information, they won't...It's as simple as that," he said. The leadership challenge, he added, is to find incentives to motivate and educate people to take action.

Participants also heard from a host of guest speakers, including Chief Edgar MacLeod (President of the CACP), and

Quebec Public Security Minister Jacques Chagnon, who both emphasized the need to overcome traditional obstacles to information sharing.

Overarching the discussions at the roundtable and plenary sessions was a commonly voiced concern among participants that police need to take immediate action to ensure greater information sharing and interoperability in their work.

Police culture was often cited as an impediment to achieving this goal. Participants contended this was far from being an excuse to not take action, but rather that this represented an important part of the future of Canada's criminal justice system. As Toronto Police Chief Julian Fantino summarized: "We (the police) are under a microscope...(and) there will be no forgiveness for not connecting the dots."

PHOTO COURTESY OF CACP



CHIEF JULIAN FANTINO,
TORONTO POLICE SERVICE

Overarching the discussions at the roundtable and plenary sessions was a commonly voiced concern among participants that police need to take immediate action to ensure greater information sharing and interoperability in their work.

But recognizing the need for improved information sharing is only part of the challenge—implementing this kind of undertaking is a formidable task on its own. As Nicole Jauvin (former Deputy Solicitor General of Canada) noted: “The concept may be simple, (but) what we’re doing is revolutionizing the way that we track individuals and the way day-to-day decisions are made across the criminal justice system.” Roundtable participants often cited privacy, technology, standards, the need for harmonization of policies and the development of seamless systems as areas where additional work will be required before improved information sharing and interoperability can be achieved.

Current information-sharing efforts underway by police across Canada were also showcased in the panel discussions. These efforts were highlighted in remarks by a host of panelists, including Assistant Commissioner Rod Smith (RCMP), Denis Méthé (Correctional Service of Canada), Chief Brian Collins (London Police), Chief Vince Bevan (Ottawa Police), David Douglas (British Columbia Organized Crime Agency, and Superintendent Dick Grattan (Integrated Border Enforcement Team). Each panellist provided delegates with a unique perspective on the challenges of implementing a tailor-made interoperability or information-sharing solution in their respective domain.

The forum also sought direct feedback from participants. A survey was distributed asking respondents to identify the steps that the CACP needs to take to ensure better information sharing and interoperability among police and other criminal justice partners in Canada. These survey questionnaires were completed by participants and were collected and reviewed during the conference so that an action agenda could be prepared before the conclusion of the forum. The survey results were consistent with the messages that surfaced in keynote and panel discussions—most expressed a sense of urgency to address information sharing.

The following list of action items were adopted:

A) For participants and their respective organizations:

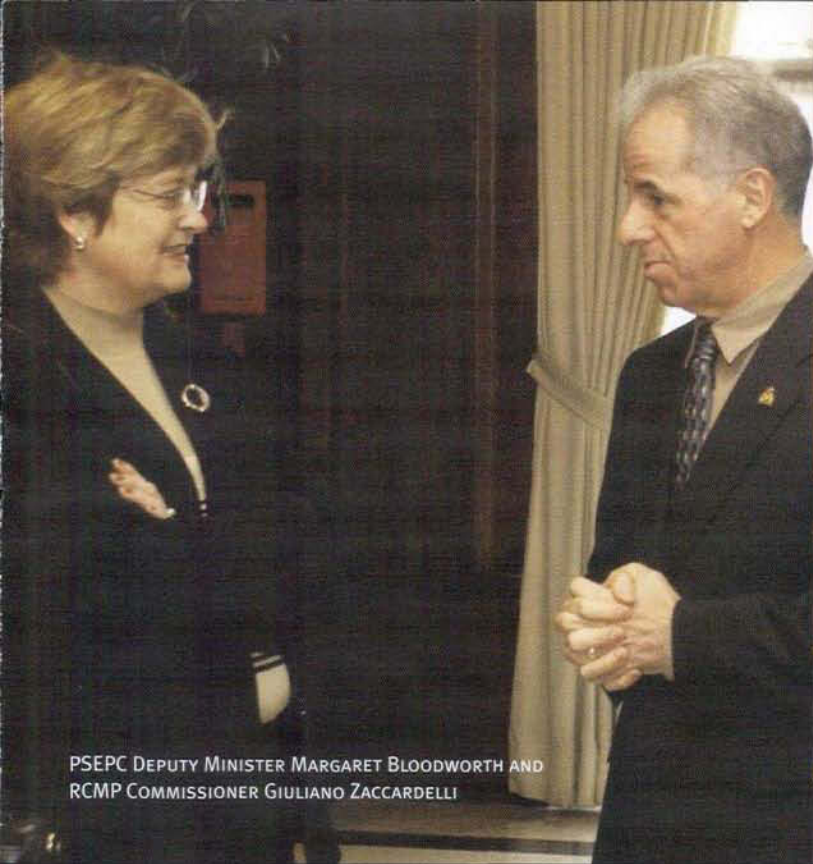
- brief the executive committee on the conference;
- conduct an inventory of information holdings as well as systems and policies on information sharing;

- identify the operational needs for information available from other agencies;
- engage in discussions with other organizations to work out interoperability issues; and
- determine a migration plan for implementing CPSIN data standards.

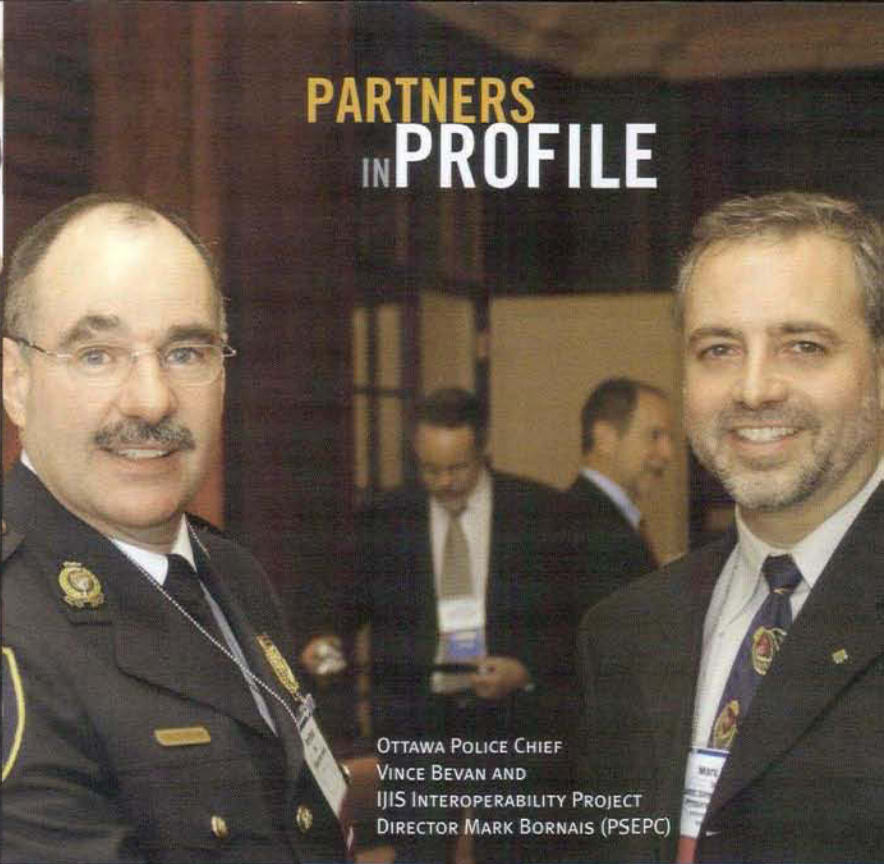
B) For the CACP:

- develop a survey to determine the status of implementing CPSIN data standards by police services and law enforcement agencies;
- establish an index of connectivity facilities and systems; and
- develop a CACP policy statement on interoperability and information sharing, and distribute it to all police services, governing authorities and conference participants.

**PARTNERS
IN PROFILE**



PSEPC DEPUTY MINISTER MARGARET BLOODWORTH AND
RCMP COMMISSIONER GIULIANO ZACCARDELLI

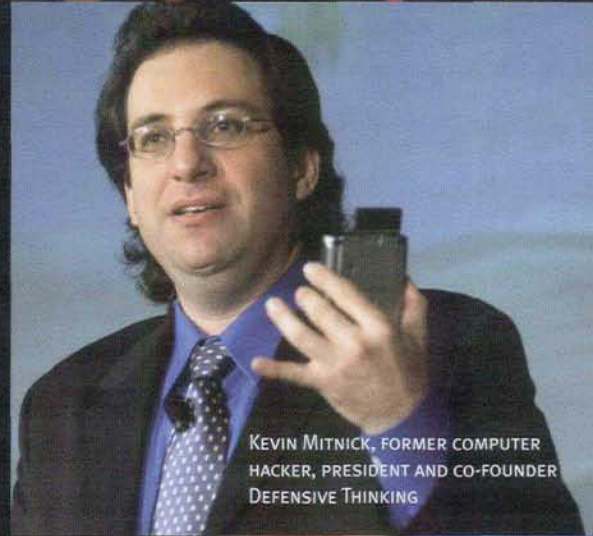


OTTAWA POLICE CHIEF
VINCE BEVAN AND
IJIS INTEROPERABILITY PROJECT
DIRECTOR MARK BORNAIS (PSEPC)

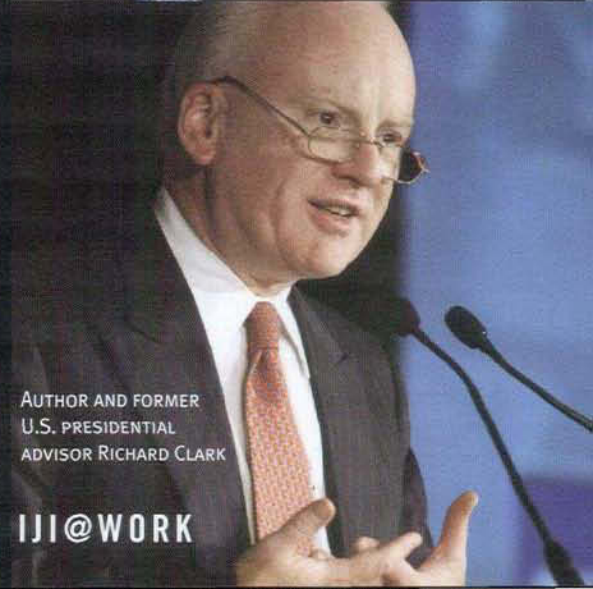
PHOTOS COURTESY OF REBOOT COMMUNICATIONS

Strategies for Public Safety Transformation 2004

Highlights from the annual international
conference on technology and
counter-terrorism



KEVIN MITNICK, FORMER COMPUTER
HACKER, PRESIDENT AND CO-FOUNDER
DEFENSIVE THINKING



AUTHOR AND FORMER
U.S. PRESIDENTIAL
ADVISOR RICHARD CLARK

PARTNERS IN PROFILE

SENIOR REPRESENTATIVES FROM GOVERNMENT, POLICE, SECURITY AND THE TECHNOLOGY SECTOR MET IN OTTAWA ON APRIL 26-27, 2004, FOR THE THIRD ANNUAL CONFERENCE ON TECHNOLOGY AND COUNTER-TERRORISM, ENTITLED *STRATEGIES FOR PUBLIC SAFETY TRANSFORMATION 2004*. PRESENTED BY REBOOT COMMUNICATIONS AND HOSTED BY THE CANADIAN ASSOCIATION OF CHIEFS OF POLICE AND PUBLIC SAFETY AND EMERGENCY PREPAREDNESS CANADA (PSEPC), THIS TWO-DAY GATHERING SERVED AS A UNIQUE OPPORTUNITY FOR SENIOR EXECUTIVES FROM CANADA, THE UNITED STATES AND ABROAD TO NETWORK AND COLLABORATE ON PUBLIC SAFETY ISSUES.



PHOTO COURTESY OF REBOOT COMMUNICATIONS

FROM LEFT TO RIGHT: JOHN PISTOLE, EXECUTIVE ASSISTANT DIRECTOR, U.S. FEDERAL BUREAU OF INVESTIGATION; MARGARET BLOODWORTH, DEPUTY MINISTER, PSEPC; GIULIANO ZACCARDELLI, COMMISSIONER, RCMP; BOB MORINE, VICE PRESIDENT AND GENERAL MANAGER, IBM CANADA; AND PHILLIP WEBB, CHIEF EXECUTIVE OFFICER, POLICE INFORMATION TECHNOLOGY ORGANISATION, UNITED KINGDOM.

Leaders from police and national security in Canada and from around the world were also well represented in panel discussions, and included the participation of RCMP Commissioner Giuliano Zaccardelli, Chief Edgar MacLeod (President, CACP), Chief Vince Bevan (Ottawa Police Service), John Pistole (Executive Assistant Director, U.S. Federal Bureau of Investigation), and Phillip Webb (Chief Executive Officer of the United Kingdom's Police Information Technology Organization). Presentations by these leaders provided delegates with vital perspectives and insight on how police can better share information on a domestic and international scale. Specific approaches to overcoming barriers to information sharing were also discussed during panel deliberations.

In keeping with the international scope of this yearly conference, delegates were treated to two special keynote addresses. The first was by Richard Clarke, the author of *Against All Enemies: Inside America's War on Terror*, and former U.S. Presidential advisor on counter-terrorism. Among the key points in his speech, Clarke emphasized that technology today affords governments unparalleled abilities and potential access, and contended that this matter should be further explored through an expanded civic dialogue.

The second guest keynote was delivered by Kevin Mitnick, an internationally known former computer hacker, who was once considered the most wanted computer criminal in U.S. history. Through a series of case studies, Mitnick provided a compelling case for why organizations need to double-up their safeguards of personal information against hackers and other intruders who seek to use that information to their advantage.

By all accounts, *Strategies for Public Safety Transformation 2004* was a great success. Based on the success of this gathering and its predecessors (held in Whistler, B.C., in 2002, and Bal Harbour, Florida, in 2003), the fourth Annual Conference is being planned for 2005 in San Francisco, California.

Details on the 2005 Conference will be available soon at the Reboot Communications website at: www.rebootcanada.com.

"We were pleased to bring this conference to Ottawa for the very first time," explained Greg Spievak, president of Reboot Communications. "Timely panel discussions and keynote speakers are hallmarks of this exclusive annual conference, and this year's gathering was no exception."

Delegates heard over 30 unique presentations by distinguished international authorities. Among the speakers representing the Government of Canada, delegates heard from PSEPC Deputy Minister Margaret Bloodworth, who provided an overview of her department and its near-term public safety priorities, including interoperability, the National Security Policy, Lawful Access, as well as measures to improve critical infrastructure and ensure cyber security. Additional in-depth information on the department's recently-launched Interoperability Project was shared with delegates in a separate presentation by Project Director Mark Bornais (PSEPC Integrated Justice Information Secretariat).

The vital importance of fostering improved interoperability surfaced at several points during keynotes and panel discussions. Speakers noted that governments in Canada, the United States and abroad must embrace the challenge of getting various agencies to interconnect information without compromising privacy or the security of their individual systems. A range of solutions in this regard were demonstrated in presentations and by numerous vendors at the conference exposition hall, including solutions such as user-authentication systems, data encryption and wireless connectivity.



A COMMON WILL TO CONNECT

UPDATE ON NATIONAL PARTNERSHIPS AND ON PUBLIC-SAFETY COLLABORATIONS BETWEEN CANADA AND THE UNITED STATES

WORKING TOGETHER AS PARTNERS, FEDERAL, PROVINCIAL AND TERRITORIAL DEPARTMENTS AND AGENCIES RESPONSIBLE FOR CRIMINAL JUSTICE AND PUBLIC SAFETY IN CANADA ARE, IN EFFECT, THE REPRESENTATION OF A *COMMON WILL* TO CONNECT AND SHARE INFORMATION IN AN EFFICIENT, RELIABLE AND SECURE MANNER.

From Nova Scotia's Justice Enterprise Information Network (JEIN) to Manitoba's Integrated Legislative Response Team (ILRT), from B.C.'s Justice Information System (JUSTIN) to Quebec's Integrated Justice Information (IJIS) Project—to name but a few initiatives—the push to achieve integrated justice information and interoperability is evident across the country.

PARTNERS IN PROFILE

Together, the achievements of partners at all levels of government demonstrate that important strides are being made to the benefit of public safety in Canada.

CPSIN partners, including Public Safety and Emergency Preparedness Canada (PSEPC) have learned much from each other, thanks to IJI-related efforts to date. Dialogue is key to ensuring that this thriving learning environment remains sustainable.

To support and promote partnerships among organizations that comprise CPSIN, the Integrated Justice Information Secretariat's Partnerships Division continues to pursue many avenues of dialogue in 2004, including:

- ongoing meetings (both ad-hoc and annual) of the Federal, Provincial and Territorial Leadership (FPT) Network, consisting of regular face-to-face and teleconference discussions since 2001 to review the status of interoperability and information sharing. The next annual meeting of this group is scheduled to take place in Ottawa in June 2004;
- the development of a *National Approach to Sharing Information*—in partnership

with federal, provincial and territorial (FPT) representatives—with a view for the FPT Ministers of Justice to formally sign a joint national statement on a national accord on information sharing;

- conducting consultations with provincial partners in Saskatchewan and Nova Scotia, to obtain their views and suggestions on a departmental policy document, *Framework for Managing Information*; and
- arranging for the participation of PSEPC Deputy Minister, Margaret Bloodworth, at an April 2004 forum on public safety and counter-terrorism, entitled *Strategies for Public Safety Transformation—Terrorism and Technology: Prevention, Protection and Pursuit* (hosted by the Canadian Association of Chiefs of Police).

Collaboration with the United States is equally important—a matter that is underscored by the Smart Border Declaration and the annual Canada-U.S. Cross-Border Crime Forum. Both countries are eager to explore interoperability issues among law enforcement departments along our shared border.

Not only is this undertaking serving to reinforce well-run security that manages the Canada-U.S. border, it is also helping to address gaps in that system. For example:

- the Canada Border Services Agency's NEXUS program for pre-approved movement of travellers is now operational at ten border crossings, and will soon be expanded to include three additional sites;
- the Canada Border Services Agency's Free and Secure Trade Program (FAST) is now functional at 12 of the highest volume commercial crossings, representing 80 per cent of commercial traffic between Canada and the United States; and
- Public Safety and Emergency Preparedness Canada will continue to explore ways to build on the successes to date, collaborating closely with the United States in a manner that is consistent with privacy concerns, human rights and Canadian law.

CONTINUED FROM PAGE 21

THE HUMAN FACTOR

Of course, everyone's appearance changes slightly between the time of one picture-taking and another. And that means that the alphanumeric sequence generated for the same individual will be different on each occasion. But Francœur says the differences are so slight that the system can calculate reasonably when it is looking at the same person.

"Through our study, we identified the impacts of nearly 20 photo characteristics on FR accuracy," he explains, "everything from luminosity to aging and facial hair. I even volunteered a picture of myself clean-shaven and one with me sporting a full beard. But the system can be configured to process those variations intelligently."

Importantly, Francœur notes that no FR system would make strictly automated decisions. If a person's image seems to match someone on a watch list in a database, a human screener is alerted to examine the matter further.

"This is an advantage, for us, over something like fingerprint technologies," says Francœur. "If you think you have a false positive—or have to verify a genuine positive match—with a fingerprint, you'd require very specialized skills. It's much easier to train people to compare and evaluate pictures."

WHAT THE FUTURE LOOKS LIKE

Through its study, the Passport Office confirmed that FR technology is mature, efficient, and advanced enough to be considered for deployment. Francœur and his project team have deposited a positive business case with the Privacy Commission for consideration.

"I'm very interested to see how the business case is received," says Francœur. "We're convinced FR will work for our requirements—will help us address real threats to Canadian security. And that is the core significant value that is being sought by all Canadian passport applicants: to hold a secure document that is internationally recognized."