JGM Information Sharing Presentation
(Bal Harbour, Florida - March 10, 2003)

Introduction

Good morning. I am delighted to be here this morning with Assistant Commissioner Tim Killam and with such distinguished guests.

First, let me say that considering the topic of this panel, it is appropriate that I am sharing the podium with a representative of the Royal Canadian Mounted Police. Under the leadership of the former Solicitor General of Canada Lawrence MacAulay, current Solicitor General Wayne Easter, and Commissioner Guiliano Zaccardelli, Canadian law enforcement has been an indispensable partner to the United States. Long before the terrorist attacks of September 11th, Canada provided consistent and invaluable assistance to law enforcement officials in the United States. And since the attacks, our nations have collaborated more closely than ever.

I greatly appreciate the opportunity to speak to all of you this morning about an issue of increasing importance to the U.S., Canada, and all nations seeking to secure their borders and protect their citizens from the threat of terrorism. When Attorney General Ashcroft addressed Congress in July 2002 on the topic of terrorism, he spoke extensively about "our most valuable resource in this new war on terrorism." Attorney General Ashcroft was not referring to bullets, guns, or handcuffs. The Attorney General was referring to information. Indeed, the ability of our law enforcement agencies robustly to share investigative information domestically and to disseminate such information to international partners may be decisive factors in the war on terror.

Information sharing is a perfect topic for this conference. It raises issues of law and policy that are currently being shaped in both of our countries by our collective counter-terrorism efforts. It also poses questions about technology and its ability to leverage law enforcement's capabilities. I plan to touch upon each of these areas in my brief address.

First, I will begin by explaining how the mission of the U.S. law enforcement community has evolved in the aftermath of the September 11th terrorist attacks and how our understanding of the role of information sharing has likewise evolved. Next, I will discuss how the U.S. government has embraced this new understanding of the pivotal role of information sharing and made necessary changes to our domestic laws, policies, and practices to advance a new paradigm of law enforcement and to facilitate domestic and international information sharing. Lastly, I will touch upon the work that we have yet to accomplish, both in the domestic and international law enforcement communities, and how many of us in this room can assist each other in improving our joint information sharing efforts.

The New Law Enforcement Paradigm: Prevention

Undoubtedly, the September 11th terrorist attacks reshaped the mission of U.S. law enforcement, perhaps forever. Before September 11th, U.S. law enforcement's mission was essentially reactive. We were principally responsible for prosecuting crime. That is, we gathered evidence about a crime that had been committed, identified and arrested the perpetrator or perpetrators, and brought them to trial in a courtroom.

Following September 11th, our responsibilities as prosecutors and law enforcement agents have been re-cast. In order to fight and defeat the threat of terrorism, the Department of Justice has added a new paradigm to that of prosecution - a paradigm of prevention. The September 11th attacks and the continuing threat of international terrorism have demonstrated that law enforcement must not simply respond, react, and punish; it must also prevent, deter, and protect.

But our government's ability to effectively prevent, deter, and protect is dependent upon our ability to exploit the information in our possession. After all, you cannot protect against the unknown. The U.S. government collects a tremendous amount of information every day. This information is collected at our borders, in our airports, on our streets, and of course from abroad. It is in the possession of agencies and entities responsible for immigration, national defense, law enforcement, and intelligence. It is also held by various sectors of the private industry. Indeed, there is a treasure trove of information potentially at our disposal, and if it were marshaled, it would have tremendous preventive and predictive value.

Harvesting all of this information is a cornerstone to our counterterrorism efforts. In the world of intelligence, there is something called the "mosaic theory." It posits that critical information may consist of seemingly inconsequential pieces of information. Each of these facts standing alone may mean nothing – a suspect may take a trip, ship a package, or open a new bank account under a different name. However, when placed in the context of other information, such innocuous facts can create a mosaic picture of plans being laid for an attack. Just like a mosaic, the true picture will not emerge unless all the pieces have been gathered and properly assembled.

Unfortunately, in the aftermath of the September 11th terrorist attacks, the U.S. government discovered that it was not terribly proficient at "knowing what it knows." Too frequently, we collected information without adequately exploiting it. Agencies collecting information failed to make links between pieces of information and failed to get that information into the hands of others who could. Improving these circumstances required fundamental reforms in the way that our government did business.

To make the necessary reforms, the U.S. government embarked upon an ambitious effort to create a new culture among all those who bear the responsibility for enforcing our laws; a culture ripe for interagency and international cooperation, innovative collaboration, and information sharing. But first, the Department had to understand what it was doing wrong.

The Department's Review of Information Sharing Shortcomings

Immediately following the September 11th attacks, the Attorney General ordered a top-to-bottom review and reorganization of the Department of Justice. Our objective was to mobilize the resources of our law enforcement and justice system to meet a single, overarching goal: to prevent future terrorist attacks on the United States and its citizens.

We discovered that artificial legal barriers had needlessly separated our law enforcement and intelligence communities. Because of then-existing U.S. law and policy, intelligence gathering was artificially segregated from law enforcement, effectively barring intelligence and law enforcement communities from integrating their resources. Decades-old policies had erected walls between different government agencies, hindering them from cooperating in the nation's defense. The FBI and the CIA were restricted from sharing valuable information with each other. And as limitations on information sharing tightened, cooperation decayed. As information restrictions increased, intelligence capabilities atrophied.

We also discovered that a culture of non-cooperation encouraged federal, state, and local law enforcement agencies to work in a disjointed fashion, even when they had a common goal. This shortcoming was emblematic of a bigger problem: parochialism. Federal, state, and local agencies were focused only on their narrow tasks and their particular constituents rather than on the broader mission of protecting the entire country and all of its citizens. Too often they operated in their respective boxes and did not pool resources and capabilities.

We also found that our use of technology, which should have improved our analytic and information dissemination capabilities, had instead resulted in balkanized pools of information locked in government agencies, which were using proprietary computer systems unable to interface with other computer systems. Technology had become our foe rather than our ally because proper strategic planning had not been conducted to ensure interoperability and compatibility across the government.

Based on the Department's review, we concluded that our law enforcement and justice institutions - and the culture that supports them - had to improve if we are to protect innocent Americans and prevail in the war against terrorism. We had to create a new system, capable of adaptation, secured by accountability, nurtured by cooperation, built on coordination, yet still rooted in and abiding by our Constitutional liberties.

One of the first steps was modifying the law to eliminate unwarranted legal obstacles to law enforcement practices and which were consistent with the new paradigm of prevention.

How the USA PATRIOT Act changed domestic information sharing practices

The Department's post-September 11th agenda for amending U.S. law covered many areas of enforcement: for example, immigration, money laundering, and electronic monitoring. Yet,

many of the changes to law that we sought specifically involved the handling and dissemination of law enforcement and intelligence information. During the last year and a half, we have eliminated or reduced many longstanding legal barriers to the flow of information within the government. We have also encouraged public-private partnerships that have required us to re-think how we regulate access to information. It is particularly significant that we have done so without compromising national security by needlessly disclosing sensitive information and without upsetting important limits to governmental authority.

In the immediate aftermath of September 11th, the Department worked closely with Congress to pass the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, better known by its acronym the USA PATRIOT Act, to address the threat of international terrorism. Notably, Congress agreed with the Department's assessment that information sharing was among the problems that had to be addressed immediately by legislation. The USA PATRIOT Act took the unprecedented step of mandating that the Attorney General and the Director of Central Intelligence create procedures for the exchange of information between the intelligence and law enforcement communities. The USA PATRIOT Act also amended U.S. laws governing wiretaps and grand juries to eliminate longstanding provisions that prevented prosecutors and law enforcement agents from sharing information derived from those sources with other agents, investigators, and officials across the country.

Understand that permitting information sharing of wiretap and Title III information was a seismic change to law enforcement practices. Grand juries and wiretaps are among the most invasive criminal investigative techniques at law enforcement's disposal and, consequently, information derived from those sources have always been closely held. The fact that such changes were enacted, however, was testimonial to how much our mind set had changed by the recognition that we had to a better job of "connecting the dots" to prevent another major terrorist attack.

The USA PATRIOT Act's information sharing provisions were a welcome start to breaking through the information logjam. However, the reform of information sharing practices did not end there.

How the Homeland Security Act of 2002 Changed Domestic and International Information Sharing Practices

In November 2002, President Bush signed legislation that took the next logical steps in advancing information sharing efforts, both domestically and internationally. The Homeland Security Act of 2002 established the Department of Homeland Security (called "DHS" for short) whose mission is to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur.

The Department of Homeland Security is focused on the notion of fusing information

collected from all varieties of sources: all federal agencies across the government (that is, law enforcement, intelligence, immigration, national security, military); state and local governments; the private sector; and the public. The same emphasis on pooling valuable intelligence also led President Bush to announce in his State of Union Address in January 2003 that he had instructed the Director of Central Intelligence, the Director of the FBI, working with the Attorney General, and the Secretaries of Homeland Security and Defense, to develop the Nation's first unified Terrorist Threat Integration Center. This new center will merge and analyze terrorist-related information collected domestically and abroad in order to form the most comprehensive possible threat picture.

The Homeland Security Act also removed additional legal restrictions that had prevented the dissemination of certain types of law enforcement information to state and local agencies. In addition to sharing information more robustly internally, the federal government is now building bridges to state and local governments.

Likewise, the Homeland Security Act amended the law to recognize that the battle against terrorism was global. You may recall that the September 11th terrorists trained in Afghanistan, planned their operation in Europe and elsewhere, financed their activities from the Middle East, and executed their attacks in the United States. To effectively combat and eradicate groups like Al Qaeda, we realized that we had to enlist the assistance of our international allies and had to be able to share our information with them. So, the Homeland Security Act re-wrote laws governing the dissemination of some information to foreign law enforcement officials. For the first time, U.S. law permitted the dissemination of wiretap and grand jury information to foreign law enforcement for official use.

While such changes to U.S. law will undoubtedly advance our counter-terrorism efforts, we expect that they should also benefit many of our other crime fighting efforts. For example, the narcotics trade, identity theft, organized crime, and human trafficking are also all global problems that will require global solutions. The changes to U.S. law that I just mentioned will be as helpful to combating these crimes as they will be battling terrorism.

The growth of technology used to perpetrate crimes also dictates an international approach to law enforcement cooperation and information sharing. In this new age, when crimes can be planned, contraband can be instantly transported, and illicit funds can be anonymously transferred across the borderless expanse of cyberspace, we no longer have the luxury of simply attempting to control crime within our borders without looking beyond them.

Successful International Information Sharing Efforts

The increased emphasis within the U.S. law enforcement community on international information sharing efforts has already borne fruit. Of course, the U.S. continues to have successful information exchange with Canada. From the table top exercises in which our countries have jointly participated, to the help we have given each other through the Mutual Legal

Assistance Treaty process, to the informal investigator-to-investigator assistance that occurs everyday between the law enforcement agents of our countries, information sharing and international legal cooperation between U.S. and Canadian law enforcement officials is increasingly robust. This cooperation is exemplified by the Cross Border Crime Forum, which, under the leadership of the Canadian Solicitor General and the U.S. Attorney General, every year brings forth over 150 senior law enforcement officials from our countries.

Through cross-border information sharing efforts like the Cross Border Crime Forum and the "Smart Borders Initiative," we are working jointly to protect our citizens by safeguarding our borders. Through the newly created joint Internet Fraud Crime Complaint Center effort, our law enforcement agents will be able to search for trends in Internet crimes reported in Canada and the United States.

While our efforts with Canada have been fruitful, we are also extending our law enforcement information sharing efforts around the globe. For example, law enforcement agencies across Europe have joined with the United States to form partnerships that have enhanced the security of all our nations. Let me cite a few examples:

- We have reached landmark information sharing agreements with EUROPOL.

- The United States has forged additional ties of cooperation with Switzerland, including a special "working arrangement" with the Federal Department of Police and the Swiss Antiterrorism Task Force.

- Scores of formal U.S. requests for evidence needed in a wide variety of terrorism investigations - from bank records to witness interviews - have been granted promptly by countries across Europe.

- We are also in the process of negotiating an unprecedented judicial cooperation agreement between the United States and the European Union.

Our partners in the war on terrorism extend far beyond Europe. We are also working hand in hand with law enforcement officials from China to Pakistan to Colombia. Our worldwide coalition has achieved unparalleled police-to-police cooperation among different national law enforcement agencies.

Technology and Information Sharing

Since one of the themes of this conference is technology, let me say a word about the critical role that technology plays in facilitating information sharing. I mentioned earlier that U.S. agencies were failing to leverage technology to make the best use of computer-aided analysis and dissemination. Software and hardware incompatibility prevented many law enforcement agencies from sharing data. Some of these compatibility problems were symptomatic of longstanding

rivalries that existed within the federal law enforcement community – the parochialism I mentioned earlier. Others were merely a product of poor strategic planning and a failure to anticipate the growing importance that a common information and technology infrastructure would play in modern law enforcement.

In any event, hardware and software compatibility is no longer an afterthought in our strategic planning. Rather, it is a prerequisite. We work closely with our information technology staff and with private industry to develop systems that will be flexible, expandable, and compatible. We have far to go – bringing all of the government up to grade is a serious challenge - nonetheless, there is a new attention to this issue and an almost universal recognition of its significance.

We have also moved to remedy technological shortcomings in our information gathering capabilities. Terrorist organizations have increasingly used technology to facilitate their criminal acts and hide their communications from law enforcement. Intelligence gathering laws that were written for the era of land-line telephone communications are ill-adapted for use in communications over multiple cell phones and computer networks. We have created a more efficient, technology-neutral legal standard for intelligence gathering, ensuring law enforcement's ability to trace the communications of terrorists over cell-phones, computer networks and new technologies that may be developed in the coming years.

Steps Ahead and Conclusion

As I reflect on how far we have come in planning and implementing information sharing efforts, I also recognize how far we still need to go. Unfortunately, as we all know, despite substantial improvement, effective, seamless information sharing is still more a vision than a reality, especially in regard to international information sharing efforts. The seeds of change have been planted, and we are just beginning to harvest the fruits of our labors. While I am optimistic that we are on the right path, I believe that furthering our efforts will require the assistance of people such as you sitting in this room.

I have talked about the important role of technology in information sharing. However, we must recognize that what stymies adequate information sharing is not primarily a lack of technology. After all, the technology for information sharing exists now and is, for the most part, readily available. So why is it that some of the our domestic and international information sharing efforts still lag behind where they should be? Why are our law enforcement entities not making the most of collaborative arrangements that would most likely be beneficial to all who participate?

I believe that three factors principally shape the behavior of the law enforcement community. First, there is the law, which is the vehicle through which our courts and legislature dictate what law enforcement is permitted to do. Next, there is policy, which entails the law enforcement agencies promulgating rules and regulations to shape their own conduct. Lastly, and in my opinion most significantly, there is the culture of the law enforcement community. The

culture of law enforcement is a collective product of the attitudes of the men and women who actually conduct the investigations and walk the beat.

Among these three factors that shape the behavior of law enforcement, I believe that the culture of law enforcement is the most difficult element to change. We have seen changes in the policy and the law concerning information sharing. After all, laws and policy can be rewritten overnight. Congress can vote to pass new laws and an agency can amend its own policies with the stroke of a pen. However, the culture of law enforcement is much more difficult to alter.

What will it take to change the culture of law enforcement to make it more receptive to information sharing? First, we must build a solid foundation of trust. To truly collaborate, law enforcement must be shown that their respective investigations and prosecutions will not be undermined or endangered by sharing information with other agencies and countries. They must also be shown that such efforts add value to their investigations.

One of the best ways that we have found of fostering this type of trust is through the collocation of investigators. Currently, the FBI has liaisons from the U.S. Customs Service, the U.S. Secret Service, the Department of Defense, and many other federal investigative agencies. These liaisons work in the same offices at FBI Headquarters, where they have online access to their own respective agencies' databases and access to the FBI's databases. President Bush's plans for a Terrorist Threat Integration Center that I mentioned earlier are premised upon the same idea: placing FBI and CIA analysts in the same building to promote the free flow of information. The increasing use of joint task forces comprised of investigative agents from federal, state, and local governments has also enjoyed great success. Through such collocation arrangements, strong working relationships have been built that can provide the required foundation for a freer exchange of information.

Another important factor to changing the culture is leadership. The message that we have a new way of doing business must come from the top down. Managers must acknowledge and reward sound information sharing practices in their agencies and discourage the type of parochialism that has failed us in the past. FBI Director Robert Mueller and CIA Director George Tenet have repeatedly, unequivocally, and publicly encouraged the type of collaborative approach to information sharing between the law enforcement and intelligence communities that has eluded us in the past.

Lastly, while I do not wish to overemphasize technological barriers to information sharing, I would note that information sharing is more likely to happen in direct proportion to the ease with which it can be effectuated. Technology can make the transmission of information simpler through the use of secure, encrypted network-based information systems. However, it is first necessary for there to be some centralization of information. From these hubs of information within our countries, information can be passed to other international hubs, which could in turn be responsible for properly disseminating to law enforcement domestically.

I thank you for this opportunity to speak to you today. I believe that we are currently on

the road to meaningful information sharing, but that it is a journey that has just begun. I look forward to working with you to rise to this responsibility. I am happy now to take any questions that you may have.