Notes for Paul E. Kennedy, Senior Assistant Deputy Solicitor General

National Policy Research Conference
Future Trends: Risk

Ottawa Congress Centre
October 23-25, 2002

"Risk and the Intelligence Services"
Concurrent Session A1 (Capital Hall 1)
Thursday, October 24, 2002 - 10:45 a.m.-12 noon

Chair: Margaret Purdy, OCIPEP
Panelists: Paul Kennedy, Solicitor General Canada
Garry Loeppky, RCMP
Martin Rudner, Carleton University

"Security Intelligence – A Risk Management Enterprise"

There is no realistic number of intelligence personnel or financial resources that would ensure that all possible scenarios involving threats to national security at any given time are covered. The task of addressing the spectrum of potential threats involves on-going threat and risk analysis, priority setting and the flexible application of available resources.

For this reason, risk management of intelligence work requires "best efforts" in terms of 1) a regular review of possible and existing threats; and 2) continuously evolving approaches to deterring those threats.

My presentation will include:

- A brief history of CSIS and the regular adjustment of its intelligence priorities over the past almost 20 years;
- How the world has changed since September 11 and today's realities;
- The current government-wide approach to security and intelligence risk assessment and management at the political and senior officials level;

- Operational considerations;
- The need for continual co-ordination and co-operation at senior decision-making, policy framework and operational levels.

In conclusion, I will emphasize the importance of achieving the best balance between private rights and public expectations (essentially, zero tolerance) with regard to personal safety and national security, a delicate and often controversial process that is an essential feature of risk management in Canada today.

Let me begin by going back to my initial comments to make some general points about the nature of intelligence work.

Intelligence work involves a constant, even daily, reassessment and evaluation of risks to our national security and our public safety. In essence, the work of our intelligence services is a risk-management enterprise like no other I can think of. Like all public services, intelligence work requires an on-going evaluation of "needs" and "wants" in terms of financial support – from both administrative and operational perspectives. This will entail, therefore an allocation of resources, presumably based on the evolving assessment of risks and possible outcomes.

It is important to point out, however, that there is no realistic allocation of resources that would ensure that all possible scenarios involving threats to national security are covered. Our society should not expect, nor would it accept, an intelligence service dedicated to a "zero tolerance" approach to the management of potential threats. The costs to our rights enshrined in the *Charter*, as well as to the privacy rights of individuals, would just be too high.

The task of addressing the spectrum of potential threats involves on-going threat and risk analysis, priority setting and a flexible approach to allocating available resources. Obviously, over the past ten to fifteen years this task has been approached differently

depending on the circumstances of the global, North American and Canadian security environments. For example, before the end of the Cold War, in the early years of CSIS, the ratio of CSIS' operational resources was weighted 80/20 in favour of counter-espionage initiatives. This ratio was reversed, during the 1990s, to 60/40 in favour of counter-terrorism.

To get a better sense of the changes in the security environment over the past several years, it is interesting to look in more detail at the events and trends which have shaped the focus of CSIS' efforts over time. For example:

- In 1985, the Air India disaster claimed 329 lives.
- In 1989, the Berlin Wall fell and the Warsaw Pact effectively collapsed.
- In 1991, the former Soviet Union dissolved, its successor states faced ethnic and political instability, including civil war in Yugoslavia, all of which had a spill-over effect on Canadian émigré communities; the Persian Gulf War and other conflicts in Africa and the Asian subcontinent created mass migration and refugee movements; and, a number of developing countries were seen to be emerging nuclear nations, military stockpiles became available on the open market and nuclear scientists and their expertise were being exported from the former Soviet Union.
- In 1992, CSIS reported that most terrorist threats originated from volatile situations abroad, such as Sikh and Tamil terrorism and terrorist activities in the Middle East, Armenia and Northern Ireland; Russia's and China's intelligence services remained active against Western interests; and right-wing extremism in parts of Europe (as well as in Canada) remained a source of concern.
- In 1993, Russia and China continued to seek technological parity with the West, particularly as regards technology for military purposes; the World Trade Center in New York was bombed by Middle Eastern terrorists; and worrisome trends such as the proliferation of weapons of mass destruction and missiles with which

to deliver them and the internationalization of organized crime affected the assessment of threats facing Canada.

- In 1994, CSIS reported that it no longer investigated many countries that once were a concern, and, in fact, CSIS began to develop liaison relations with the intelligence services of former Warsaw Pact countries. However, international terrorism continued to affect CSIS priorities as a result of such incidents as a bombing in Buenos Aires, two car bombings in London, England and the hijacking of an Air France jet in Algeria.
- In 1995, the IRA exploded a bomb in London which ultimately rendered the ceasefire a shambles; Algeria dissolved into civil strife, triggering a wave of terrorism against foreigners and France; in Sri Lanka, a secessionist battle led to a powerful truck bomb that killed more than 50 people; and a nerve gas attack in a Tokyo subway by the Aum Shinrikyo cult killed 12 and injured at least 5,500. (The deadly nerve agent, Sarin, had been previously identified by proliferation experts as one of the most likely agents to be used in a terrorist attack.)

By 1996, CSIS reported that the threat from international terrorism in Canada resulted from homeland conflicts, and many of the world's terrorist groups had established presences in Canada in order to engage in a variety of activities in support of terrorism, including:

- Providing logistic support for terrorism outside Canada;
- Developing the potential for terrorist actions in Canada;
- Fund-raising, advocacy and information dissemination;
- Intimidating Canadian citizens in émigré communities;
- Providing a base for terrorists;
- Arranging transit to and from other countries; and
- Raising money through illegal activities.

And by the year 2000, resources were shifted from areas of lesser threat so as to intensify investigations related to Islamic extremism. This work now includes pursuing leads

regarding networks being put in place to support a range of terrorist activities. It is clear from this review of global terrorism and related Canadian concerns that shifting priorities and the reallocation of resources based on threat assessment and risk management are a continual exercise to maximize the potential of all available resources.

I should add, in terms of resource allocation, that part of the exercise of risk management depends on the financial resources available, and this also has shifted over time in the same way as the potential threats assumed different forms. For example, as a result of a Program Review exercise in the early 1990s, CSIS' budget decreased by almost 35 percent between 1993/94 and 1997/98. This also affected CSIS staffing to the extent that there was a 27 percent reduction between the years 1992 and 1997.

This overall decrease in resource allocation to Canada's primary intelligence service occurred in the years immediately following the Gulf War, an increase in terrorist activity in the Middle East and elsewhere, the bombing of the World Trade Centre in New York, and growing concerns about the proliferation of weapons of mass destruction. And although there were minor increases in CSIS funding again by 1999, it was only after September 11, 2001, the resourcing of intelligence work was significantly increased to levels commensurate with the nature of the threat.

The events of September 11th precipitated not only a significant shift in the global threat level, but also in terms of the ensuing response of CSIS. Although public safety and safeguarding against the possibility of a terrorist attack occurring in, or originating from, Canada were already the highest priorities of CSIS (Sunni Islamic extremism was an important focus of CSIS' counter terrorism program since the late 1990s), following the attacks in the U.S., it was necessary to adopt a heightened operational stance in order to further assess the threats posed by Sunni Islamic extremists in Canada, to closely monitor the potential for retaliatory attacks against the U.S. and to assist the U.S. agencies in their investigations.

Accordingly, in October, 2001, the Government announced an interim allocation of $10 million to help cover the immediate costs of the intensified efforts of CSIS to monitor and investigate potential terrorist threats. In addition to this immediate response as part of the on-going risk management responsibility of the Government as a whole, the federal budget of December, 2001 provided CSIS with a 30 percent increase to its overall budget over a five-year period to ensure that CSIS has all the staff and technology it needs for its counter terrorism efforts.

Since September 11th, Canada's attention to ensuring Canadians' safety and sec urity has been brought into focus. However, risk management in relation to intelligence work is only one piece of the government's overall risk management effort. Immediately after September 11th, the Canadian Government took action to counter the treat posed by terrorism and to enhance security both domestically and abroad. Part of this approach involved enhanced information sharing and co-operation, again at both federal/provincial/territorial and international levels of collaboration.

The existing government-wide approach to security and intelligence risk assessment and risk management is structured to reflect Canada's parliamentary system, in that it is the Prime Minister of Canada who is ultimately accountable to Parliament and to the people of Canada for the security of the country. The Prime Minister, therefore, provides broad guidance to the security and intelligence community within the federal government.

Within the Cabinet framework, Ministers collectively establish intelligence priorities for the security and intelligence community at an annual (or as needed) Meeting of Ministers on Security and Intelligence, usually chaired by the Prime Minister. In addition, through discussions at regularly scheduled Cabinet committee meetings, Ministers also provide direction on major policy and resource issues related to security and intelligence, such as airport security, the sale of Canadian encryption technology abroad, or funding for the community's action against organized crime. And since September 11th, an ad hoc

Cabinet committee has met regularly to address immediate and longer-term needs in the fight against terrorist activities here in Canada, within North America and abroad.

Although no single Cabinet Minister is fully responsible for the federal government's security and intelligence community, there are a number of Ministers who are accountable for the activities of the organizations that report to them. They include the Solicitor General, who is Canada's lead Minister for counter-terrorism. This role reflects his responsibilities for both the Royal Canadian Mounted Police and the Canadian Security Intelligence Service.

For example, the Solicitor General is responsible for co-ordinating Canada's response to domestic terrorist incidents, and specifically, he is responsible for maintaining a National Counter-Terrorism Plan. This Plan is not new – it was approved by the government in 1989, following a recommendation by a Senate Committee that the Department of the Solicitor General strengthen its role as a co-ordinator of national counter-terrorism arrangements. But since September 11th, its relevance has been brought into sharp focus.

The essence of this Plan is its risk-management function at the operational level. Its overall aim is to ensure the co-ordination of counter-terrorism roles, responsibilities and resources of all federal departments and agencies with security and intelligence functions, as well as other levels of government and law enforcement in Canada's provinces and territories.

The Department of the Solicitor General reviews this Plan on a regular basis (the last major review, with the addition of a chemical, biological, radiological, nuclear (CBRN) component was completed in 2000), again reflecting the need to make adjustments in accordance with the assessment of risks as they evolve over time. At this time, we are carrying out another review of the Plan, which will encompass lessons learned in the wake of September 11th and the impact of Canada's anti-terrorism legislation, which was passed in December 2001.

The *Anti-Terrorism Act* was enacted to help ensure that Canada can play its part in the global effort to disable and dismantle terrorist organizations. This legislation created, among other provisions, a definition of "terrorist activities" and enforcement measures to take action against those responsible for terrorist acts.

It gives law enforcement and intelligence agencies new investigative tools to make the use of electronic surveillance against terrorist groups easier. And, within carefully defined limits, it includes provisions which allow for the arrest, detention and imposition of conditions of release on suspected terrorists, as well as requiring individuals who have information on a terrorist group or offence to appear before a judge to provide that information.

The Act also ratified two United Nations anti-terrorism conventions (suppression of terrorist financing and suppression of terrorist bombings). These kinds of international initiatives and co-operation have become even more important in the 21st century in terms of the globalization of terrorist activities and the fight against terrorist fund-raising activities.

An integral part of the *Anti-Terrorism Act* is the Government's ability to create a "list of entities" as a very public means of identifying a group or individual as being associated with terrorist activity. In July 2002, the Solicitor General announced the listing of seven groups, which, under the new law, became liable to have their assets frozen and potentially seized and forfeited. And there are severe consequences and heavy penalties for persons and organizations that knowingly support these entities or deal in the property or finances of these listed groups.

These measures will ensure that financial and other support mechanisms used by terrorist organizations are less available and better scrutinized by law enforcement, intelligence agencies and other regulatory bodies. This kind of formal legislative response is

a significant part of the government's risk management – that is, to deter potential threats against Canadians, both here and in other parts of the world, as much as is possible, before the terrorist act occurs.

Another important aspect of risk management is ensuring that our counter-terrorism response capability involves a regular cycle of training activity to generate and maintain a high level of awareness and to assess those arrangements so that they are adapted as necessary in keeping with the terrorist threat environment. This response capability also requires that we are regularly improving and refining our co-ordination mechanisms, across government, with the private sector and with the international community.

For example, one particular aspect of the terrorist threat that has come more to the forefront in the past few years is the threat of chemical, biological, radiological and nuclear (CBRN) terrorism. As we are all well aware at this time, terrorists strive continuously to arm themselves with sophisticated weaponry and technology. Clearly, this threat is a source of deep and abiding concern, and in late 2001, the Canadian government allocated significant funding to improve our national capacity to respond to such threats.

These examples of risk assessment and management, at different levels of government, are important illustrations of the links between the intelligence, law enforcement, critical infrastructure protection agencies and military preparedness. This is not to say that each institution across government does not have its own specific approaches and priorities. But it is necessary that each of these areas conduct its own risk assessments as part of an overall collaborative approach.

In addition to the Solicitor General, a number of other Ministers have key roles in the overall government management of security and intelligence matters. They include: the Deputy Prime Minister, who has the specific responsibility for security and intelligence-related concerns involving Canada-U.S. relations (in particular, the Smart Border

Initiative), and the Ministers of Foreign Affairs, National Defence, Citizenship and Immigration, Justice and Transport. The Privy Council Office's Security and Intelligence Co-ordinator, along with the Security and Intelligence and Intelligence Assessment Secretariats, also play an important role in the government-wide communication, consultation and co-ordination effort.

The government's approach to public safety and national security reflects a recognition that risk management must not occur solely on a unilateral basis within agencies and departments, but should reflect our growing understanding of the complexity of the new global realities in terms of terrorist activities and the potential for catastrophic outcomes. And at a broader level, national security, and the intelligence work that is an essential first line of defence, is increasingly affected by and dependent on factors outside the direct control of the federal government, and often, in fact, outside our borders.

Another aspect relevant to the discussion of risk management in the intelligence community is the issue of secrecy. The ability to conduct at least a part of intelligence work without full disclosure is an essential feature of this craft. And assessing risk in the intelligence-gathering framework must incorporate into that process the degree to which some of the work must be conducted in secret.

There is a constant tension within the risk assessment process between the importance of secrecy in the interests of the best possible intelligence gathering and the importance of transparency in the larger sense of public safety. It is clear that the intelligence service must consider possible adverse consequences of transparency in assessing risk. This aspect of risk management in intelligence work is neither popular nor well understood.

Canadians are shown in polls to have demanding expectations of those responsible for ensuring their safety and security. In Canada, even prior to September 11th, public safety and national security consistently ranked high in national opinion and priority polls, ahead of managing the economy and tax reform. We recognize that public safety is a key

element in maintaining the quality of life in our country – and just as importantly, in preserving Canada's place of privilege in the world community as one of the safest and most secure countries anywhere.

But, to complicate matters somewhat, the public now has an expectation that they have a right to be told all the facts and that open discussion is imperative in a democratic society. We understand that this is an important feature of our society and that this balancing of priorities also affects the assessment and management of risks in the intelligence community.

This has become even more of a factor since September 11, with Canadians wanting assurances as to their personal security, while at the same time, showing concern for issues of privacy and transparency. In terms of intelligence work, which traditionally has occurred within an envelope of confidentiality, the ability of state-operated agencies to control the collection, interception, use and disclosure of information is increasingly viewed as a public policy issue.

In the wake of September 11th, security concerns involving threat assessments and risk management will remain an important focus of Canadian policy-makers, but the security and intelligence community will face continuing challenges in balancing individual rights while maintaining Canada's reputation as a peaceful, safe and democratic society. The Government's approach to fighting terrorism, in part through the efforts of the intelligence community, has been and will continue to be grounded in its commitment to a balanced approach involving both individual rights and national security.

What we are encountering, interestingly enough, is that the public perception of the appropriate balancing has shifted from a personal rights focus in the time period prior to September 11th, to more emphasis on personal safety immediately after September 11th, and then, more recently, again expressing concern for an emphasis on the need for individual privacy protections.

The key task of CSIS, as our country's security intelligence service, is to anticipate change in the nature and extent of potential threats - in particular, change that may have even greater adverse consequences than we have seen or experienced before, in terms of both external and internal threats to our safety and security. This work, however, must occur within our democratic framework and institutions, even as we are faced with the realities of constant, rapid and volatile readjustments as to the potential for terrorist threats and activities.

This is all to say that the assessment and management of risk a democratic society requires us to accept that some tolerance of risk is necessary and unavoidable. The concept of "risk in the intelligence service", in essence, states the obvious, in that 1) intelligence work takes place only in the context of risk and 2) risk assessment and management in a democratic society requires a certain ability to tolerate risk in order to provide the best possible outcomes across the spectrum.

The risk that we accept is that our response will possibly be inadequate, because we also want to protect our enshrined rights and freedoms.. By this, I mean that, in a democracy like ours, citizens ultimately must buy into the government's response, which has, of necessity, incorporated the collective responsibility to tolerate some risk in order to protect our individual and personal rights.

Canada faces a world in which change occurs with ever-increasing speed. New challenges are constantly emerging, while long-standing threats remain with us. Like other parts of government with responsibility for our country's safety and securi ty, CSIS must prepare for future challenges over time, while managing existing threats at any given time. The tension between preparation for the future and the demands of the present requires that we balance the risks and benefits associated with each. Resources are always finite and hard choices, therefore, will always have to be made. And these

choices involve taking into account both more familiar risks and those that are less well understood (e.g. CBRN).

Managing risks is particularly central to CSIS' way of approaching its work. And because the relationship of security intelligence to other facets of government responsibility for public safety and national security is as complex as it is, it is important to emphasize the need for a framework to manage responses to different sources of risk. Risk related to the terrorist threat is not going away for the foreseeable future, nor likely will some of the challenges I have just outlined for you. The security and intelligence community will only benefit from a greater appreciation by our society of the nature and importance of intelligence work to our overall personal and national security.

-30-