Speaking Notes for
Margaret Purdy
Associate Deputy Minister
Department of National Defence

"Critical Infrastructure Protection and Public Safety"
Strategies for Public Transformation 2002 Conference:
Terrorism and Technology:
Prevention, Protection and Pursuit
Whistler, B.C.
April 29, 2002
www.rebootnorthamerica.com

It is difficult to characterize **anything** associated with the event of September 11 as "positive".

The human toll at Ground Zero, at the Pentagon and in Pennsylvania was staggering – as was the physical devastation.

As we moved last October into the responsive military campaign, we sent our soldiers, sailors, airmen and women to risk their lives to reduce the likelihood of more terrorism.

Yesterday, along with 16,000 other Canadians, I attended the memorial service in Edmonton for the four Canadian soldiers who died 12 days ago in Afghanistan.

While it was an emotional, sad event, almost every speaker reminded us that protecting Canada, protecting North America, promoting international peace and security are noble, core responsibilities of our governments and those who choose to serve their countries.

The U.S. Ambassador and the Chief of the U.S. Army were among those at the memorial service yesterday – illustrating the Canada-U.S. partnership in the campaign against terrorism.

While armed forces play a highly visible and vital role in that campaign, so too do many others – all represented at this conference:

- Police and intelligence agencies dedicated to understanding terrorism, preventing it

- Immigration, customs and transportation safety agencies dedicated to detecting terrorists on the move

- Financial tracking agencies dedicated to stemming the flow of money to terrorists

- Prosecutors dedicated to ensuring justice is served.

All these agencies – and the women and men who work in them – were on the job **before** September 11.

They had recognized international terrorism as a serious threat to public safety and they knew it was becoming more unpredictable, more complex.

They had had many successes in thwarting terrorism, in deporting and prosecuting terrorists.

What has happened in Canada **since** September 11 is that the entire country has recognized the reach and destructive potential of international terrorism.

Canadian public support remains generally high for the actions taken by our government – new legislation, increased funding, concrete cross-border actions and the largest deployment of the Canadian Forces since the Korean War.

I started by saying it seems incongruous – even inappropriate – to use the word “positive” in the same sentence as “September 11” or “9-11”.

But I think we must conclude that the resulting education and awareness raising of Canadians to public safety threats – and what governments are doing to counter these threats – **are** positive developments.

The terrorism threat is so serious it demands engagement and vigilance – not complacency.

September 11 has also generated public attention on the work of agencies – such as the one I lead – which focuses on preparing for the worst – preparing for the consequences of disasters, including those linked to terrorism.

Our government has recognized that a **comprehensive** public safety agenda must take this work into account – must ensure our country is as prepared as it can be to deal with the potential impacts on people and property and vital services.

Canada's approach to this work is unique and I was invited here this morning to describe that approach.

In particular, the conference organizers asked me to focus on our critical infrastructure protection work.

The phrase "CIP" is one of those security phrases that has entered many vocabularies since September 11.

Concerns have emerged about which facilities might be attractive to terrorists.

- How well protected are they?

- What more could we do?

The first step in analysing CIP is to get on the same page with respect to what we're talking about.

Critical infrastructure are those services, information systems and assets which, if destroyed or disrupted, would significantly affect the health, safety, security and economic well-being of Canadians and the effective functioning of governments.

It includes:

- transportation assets such as airports and bridges, ports, highways and railway lines
- energy installations such as oil and gas pipelines and power plants
- banking and financial systems
- hospitals and other emergency services
- telecommunications networks, and
- mission-critical government systems and structures.

In contrast to the Cold War lists of Vital Points, critical infrastructure now includes both the physical **and** cyber dimensions. Mapping that CI in both its dimensions is a huge challenge for us – as are modeling approaches which facilitate emergency preparedness.

The threat to critical infrastructure may be deliberate - as in the case of terrorist attacks or malicious hackers. Or it may arise from natural phenomena – earthquakes, floods, tornadoes, hurricanes or ice storms. Or it may simply be accidental, as in the case of industrial mishaps or technological failures.

But whatever the **source** of the threat, the **results** can be equally devastating. The outcome may be the same, whether an electrical grid is shut down by severe weather or by sabotage: you still have people without power, streets without lights and hospitals without heat.

Critical infrastructure in Canada faces more and more complicated risks today compared to the past.

It was this recognition that led the Prime Minister to take concrete action well before September 11.

He created the Office of Critical Infrastructure Protection and Emergency Preparedness - OCIPEP – in February last year and assigned us a two-part mandate:

- national leadership on critical infrastructure - **all** risks

- primary civil emergency management responsibility in the Government of Canada.

We are a civilian organization in the National Defence portfolio. Our staff numbers about 150 – and will reach about 200, including offices in all provincial capitals. We and our key partners in almost a dozen other federal government departments and agencies received long-term funding from the December Budget.

Our "all hazards" combined physical-cyber approach is unique in the world – although Sweden is adopting a similar model this year. The Canadian approach recognizes, as I said, that the outcomes of various incidents are similar and the responding agencies are often the same. But it also maximizes flexibility. It draws on the lessons learned during the Ice Storm, the Saguenay and Manitoba floods, Y2K.

In today's fluid and unpredictable security environment, we need to think differently and respond more creatively.

Importantly, in all of this, information technology – a focus of this conference - is accelerating at a breakneck pace. It was simply not a consideration in civil defence planning in the 60s and 70s. Someone has pointed out that, when you throw away one of those singing birthday cards, you're throwing away more computing power than existed in the world at the end of the Second World War.

Information technology has undeniably enriched our lives, but it also has a dark side. It has introduced unprecedented new vulnerabilities and generated new threats to critical infrastructure.

The Internet and global IT networks have enabled individuals and organizations to extend their reach further, faster and more cheaply than ever before.

This is surely one of the great ironies of the modern age. The more advanced a society becomes, the more reliant it becomes on technology which is relatively easily exploited and can be used against its well being. We've seen the damage perpetrated by young, unaffiliated amateurs such as Mafia Boy. We've seen malicious attacks launched by both sides of conflicts in the Middle East and elsewhere. Without doubt, we will now see serious cyber attacks launched in the future, including against critical infrastructure.

As computer networks become more complex and interconnected, damage to one part can quickly cascade across others, affecting almost all aspects of our lives. Electrical power is lost. Traffic lights stop. Water and sewage systems are disabled. Communications systems break down. Computers freeze. Data bases are corrupted, rendered inaccessible or destroyed. Computer-run weapons systems become inoperable. And on and on.

Critical infrastructure far removed from the site of **physical** damage can be impacted. We saw the massive telecommunications breakdown – wired and wireless – in the U.S. caused by the loss of key facilities in and around the Twin Towers on September 11.

The new vulnerabilities, if exploited, can also hurt the bottom line. American companies lost $12 billion U.S. last year due to hackers and viruses. The "Code Red" worm of last July cost the world economy as much as $2 billion in IT expenses and lost productivity.

The landscape of public safety shifted in many directions with the tragic events of September 11th. For one thing, the attacks confirmed the attractiveness to terrorists of targets chosen for their symbolic or emotional significance – not their military or strategic value.

This challenges our protection and prevention ingenuity.

And this adds up to a security environment which is fundamentally different from that which existed even a few years ago; one that calls for new thinking and new approaches.

Perhaps most importantly, this new environment has highlighted the need for leadership, coordination and partnerships - across sectors, across regions and across borders.

This is the central operating environment of OCIPEP.

We are **not** an intelligence-gathering body. We do **not** enforce laws. We do **not** regulate the protection of critical infrastructure or enforce emergency management strategies in other levels of government or in the private sector.

Rather, we act as a catalyst for action - a coordinating body that can exercise national leadership because we have a national mandate and a transnational perspective.

Key to that is developing close working relationships - partnerships - with Canadian and international law enforcement agencies, intelligence services, emergency services, and first responder communities, non-governmental organizations such as the Red Cross, armed forces as well as our provincial and territorial counterparts.

But even those public sector partnerships are not enough. Because the Government of Canada owns or controls only about 10 per cent of Canada's critical infrastructure - with the lion's share held by the private sector - we also have to bridge the traditional distinctions between the private and public sectors and recognize the common role that both must now play in preserving public safety and security.

No one level of government - and no single company or infrastructure - can protect the critical infrastructure of the nation. So we must join forces. Our job at OCIPEP is to get everyone pulling in the same direction when it comes to critical infrastructure protection and emergency management. Has it been easy? No – not always. Working horizontally is really hard. Staying in silos and stovepipes is much easier. Individual accountabilities are easier to understand than shared accountabilities.

OCIPEP has worked hard to establish strong links with the provinces and territories and the private sector and to inform them of physical and cyber threats and vulnerabilities, as well as solutions and best practices. We issued about 60 alerts and advisories last year to an e-mail contact list of about 500 recipients, and published this information on our web site.

I chaired the first ever federal/provincial/territorial meeting of DMs responsible for emergency management and critical infrastructure protection earlier this year. We recently hosted a workshop which brought together, for the first time, representatives from three key infrastructure sectors in Canada - banking, telecommunications and electricity - to discuss how we could all work better together, raise awareness, share information, make a difference.

Getting reliable information to the right place at the right time is vital if Canada's critical infrastructure is to be safeguarded. Information about cyber-based threats come from open sources in software vendor notices of faults or backdoors, for example. Or it may emerge during a police or security investigation. Or it may emerge from international intelligence-sharing networks.

We're exploring with Paul Kennedy and his team, the RCMP, CSIS and CSE innovative models for triaging this information, getting it to key stakeholders and coordinating national responses **without** jeopardizing criminal or security investigations.

We are also working to enhance the capacity of first responders in Canada to manage risks and deal with emergencies and disasters. Who can forget the heroic efforts of fire, police, ambulance and medical workers at Ground Zero?

We are allocating funds provided in last December's budget to provide first responders with training and equipment to deal with chemical, biological, radiological and nuclear attacks. The anthrax incidents confirmed the need for this. We have also helped fund HUSAR teams in several Canadian cities and we are leading discussions on a National Heavy Urban Search and Rescue Strategy for Canada.

We've led efforts on two other national strategies aimed at reducing the impact of disasters in this country – a disaster mitigation strategy and a national training strategy for emergency management. We currently offer emergency management training to about 1000 local government officials each year.

One last point on the issue of partnerships, and that's the importance of working with our American colleagues.

Oil and gas pipelines cross our shared border, as do rail lines and roads. Our electrical systems are knitted together, as are our financial, air traffic control and telecommunications systems.

Canada and the U.S. must work together to share information so that we can protect our shared critical infrastructure whether the threat is an overflowing Red River, a chemical spill or a distributed denial of service attack.

The Smart Borders Declaration signed in December recognized this - with one of the 30 actions Phil Ventura mentioned committing Canada and the U.S. to enhancing the protection of our shared critical infrastructure. We've started with the transportation sector and will move on to others in the coming months.

We've all benefited from ground breaking work led by U.S. government officials.

With so many U.S. colleagues in the room, I do want to acknowledge the pioneering leadership of the U.S. on critical infrastructure protection – starting with the Presidential Commission in 1995 and moving on to the creation of the National Infrastructure Protection Centre in the FBI, the Critical Infrastructure Assurance Office, the Cyber Security Advisor in the National Security Council and so on.

Let me close by suggesting that the greatest threat to public safety today may not be a spectacular natural disaster or a disabling cyber-based attack - **but** complacency.

The challenge for all of us - as lawmakers, public officials and public safety experts - is to set for ourselves the goal, not of continuous anxiety, but of persistent vigilance.

That means continuously reviewing our plans, updating our systems and training and testing our readiness. It means lessons learned must be lessons applied. And it means engaging the public in a way that we have never done before, keeping them informed and keeping them involved.

Let me end by commending the organizers of this conference – including my colleagues from Solicitor General Canada. Not only have they enabled us to visit the most beautiful place on earth – British Columbia – but they have also helped us see the broader picture and the wider linkages in the business of public security. Conferences like this open channels of communications and close gaps of information.

And, paramount in this new post-September 11 security environment, these gatherings illuminate the importance of teamwork not territory, collaboration not competition.

That's what the "public" in public safety expects and deserves.