



**Acting Today to Face the Threats of Tomorrow:
*Protecting our Critical Infrastructure***

Speaking Notes for
The Hon. Perrin Beatty
President and CEO
The Canadian Chamber of Commerce

National Cross Sector Forum
December 1, 2010
Ottawa

Check against delivery

I'd like to start by thanking Suki Wong for the invitation to speak with you today and Public Safety for hosting us this morning. The *National Cross Sector Forum* is an important initiative and I am very pleased to have the opportunity to discuss priority issues for critical infrastructure protection in Canada. Looking at the credentials of the people in this room, however, I am also daunted, because I realise that you are the true experts on the subject. What I hope to do is to reinforce the importance of the work you are doing and to offer a particular focus on the need for us to collaborate closely with the United States and other allies in our efforts to ensure that we are adequately protected against threats and prepared to act as problems arise.

As you are all aware, the Canadian Chamber network is the most broadly-based business organization in Canada. Many of our members represent critical infrastructure sectors—transportation, energy and utilities, finance, health, communications and information technology, food, manufacturing, and water.

Given the scope of our membership and of their reliance on a dependable, well-functioning infrastructure, the Canadian Chamber views the protection of critical infrastructure as an important initiative and we welcomed the announcement of *Canada's National Strategy and Action Plan for Critical Infrastructure*.

Canada's critical infrastructure sectors are vital to the health and security of our society. However, Canada's critical infrastructure remains vulnerable to man-made and natural disasters. Disruptions of critical services can have catastrophic effects on an economy and on a society - including loss of life, destruction of property, loss of public morale and confidence.

The interdependency of many critical sectors means that a single disruption can ripple across numerous areas of economic activity. It is a two-way street: the goods and services provided by one critical infrastructure sector are vital for the functioning of other important areas. Take, for example, this summer's power outage in Toronto where a fire at the Manby transformer station cut power to more than 200,000 customers and resulted in severe transit disruptions

throughout the city. This relatively minor outage underscores how the disruption of one piece of critical infrastructure can have widespread effects on other areas.

As a result of these interdependencies, it is vital that all levels of government and critical infrastructure providers collaborate to mitigate potential risks and to develop recovery plans in case of emergencies. The *National Strategy and Action Plan for Critical Infrastructure* creates an important framework for protecting critical infrastructure in Canada. The Canadian Chamber of Commerce was pleased to see that the *Strategy and Action Plan* recognized that the responsibilities for critical infrastructure protection must be shared by all levels of government and must involve the infrastructure owners and operators. No organization in Canada has the capacity to address the risks to national security and prosperity without support from relevant stakeholders.

It is also important for us to remember that, in today's world, disruptions of critical infrastructure can rapidly spread across international boundaries. We quickly saw how interdependent we are

during the great blackout in the summer of 2003. An estimated ten million people in Ontario and 45 million residents of eight U.S. states lost power when a tree came into contact with a transmission line in Walton, Ohio.

This interdependence, which spreads far beyond the electrical grid, means that for Canada, we cannot protect our critical infrastructure without collaborating closely with our international partners - the United States in particular. In many cases, disruptions of critical infrastructure can have direct impacts on communities and businesses on both sides of the Canada-U.S. border.

An obvious example would be if the Ambassador Bridge between Detroit and Windsor was seriously damaged. Not only would the most important border crossing be closed, but so would the waterway beneath it, sealing off Chicago, Thunder Bay and Milwaukee from their access to the St. Lawrence Seaway.

As another example, the creation of an effective pandemic plan requires close cooperation with our southern neighbour. Concerns about a flu pandemic on the scale of the 1918 Spanish flu are growing. An outbreak of this nature would cause widespread illness and quarantine. With a large proportion of the workforce out of commission, productivity would decline, supplies would run out, economic activity would slow and our countries' populations would suffer greatly. Last year, the world watched as the H1N1 virus spread with startling speed. We were fortunate that the outbreak was less serious than we had feared but the threat of another pandemic is real. The physical infrastructure may be left intact by a pandemic, but the people needed to make it work may be sidelined. If our transportation, communications and financial infrastructure cannot be properly staffed, they will soon descend into disorder and the effects will cascade throughout our economy.

One of the greatest challenges for pandemic planning is ensuring that citizens and businesses are prepared for such an emergency. While large firms often have the ability to allocate resources to risk management and pandemic planning, many small and medium sized

enterprises lack this capacity. That is why the Canadian Chamber of Commerce partnered with the International Centre for Infectious Diseases to provide free tools to help small businesses prepare for pandemics. Given the integrated nature of the North American supply chain, Canada must work with our allies to develop a continent-wide pandemic plan. We must also collaborate with groups like the World Health Organization to prevent or contain outbreaks as cases arise.

As you know, Canada and the United States share a special relationship that is the envy of the world. Our close partnership is much more than an accident of history and geography. We benefit from a common environmental inheritance which is threatened by common problems like pollution and climate change. We share a common language, values, family ties and long-standing business relationships. Our economies are highly integrated.

All of these factors and more have made North America a single community. We are not simply cohabitants on a continent; we share responsibility for its defence. Our unique relationship with the U.S. has resulted in some of the most effective cross-border arrangements

in the world. The success of NAFTA and NORAD are perfect examples of what we can achieve when we work together. I firmly believe that the protection of critical infrastructure is another area where the security of our citizens depends upon our ability to work collaboratively.

The security threat to North America is real. It includes most man-made and natural dangers. Canadians must take security seriously, not because it is the price the Americans demand if we want to trade with them, but because large numbers of our own citizens may lose their lives if we are negligent. Not only have we been targeted by terrorists, but we must also be prepared to face the challenges presented by aging infrastructure and a changing environment.

As long as the United States feels that Canada cannot adequately provide American security, the Americans will continue to fortify the border. The United States is Canada's largest trading partner and together we enjoy one of the most prosperous trading relationships in the world. In 2008 the total trade between our two countries was worth more than \$676 billion—that's more than one million dollars a

minute, 24 hours a day, seven days a week. Eight million jobs in the U.S. and three million in Canada depend upon the economic relationship. We are each other's primary trading partner. Our systems are so intertwined that we don't merely trade—we actually *build things together*. But, as the smaller economy Canada will always pay the higher price for an inefficient border.

Indeed, many manufactures are shifting from a just-in-time to a just-in-case case delivery model. Today, companies cannot rely on an open border. This new reality means that they are more likely to relocate their operations to be closer to the customers. In most instances, this means moving south.

The Canada-U.S. border is a piece of infrastructure critical to the health of the Canadian economy and must factor prominently in any critical infrastructure protection strategy. The *Canada-U.S. Action Plan for Critical Infrastructure* announced earlier this year is a welcome step in the right direction. This plan lays the groundwork for a comprehensive and joint approach to critical infrastructure

protection by seeking to facilitate dialogue and improve collaboration between relevant stakeholders on both sides of the border.

Because we share a common frontier, we need to reach a common understanding and develop a common approach to border management. Our interests are already too commingled for us to have any other option.

I know that the issues are complex and nuanced, but we need to go beyond nuance and address some very basic questions about how we want to manage our bilateral relationship and protect our citizens. Canada has a strong and urgent interest in rethinking our border. If we continue to see it primarily as a wall between our two countries, Canada will be left pleading with the Americans to make the 49th parallel less sticky, less thick, and less costly. This means that we will continue to search for ways to administer obsolete infrastructure and to make misdirected policies work. Today's border has been designed to address yesterday's problems and this outdated and cumbersome system is a serious burden to legitimate trade and travel.

Until now we have been trying to manage the border by doing essentially the same thing as we have done the year before but more efficiently. Given the constantly shifting nature of the security threats we face, this strategy will get us nowhere. We need to reclassify the border as a piece of critical infrastructure and a process instead of a place. This can be accomplished by pushing out our borders through an intelligence-based approach to border management. I believe Canadians understand why it makes sense to leverage North America's geography to our advantage. They also understand that, when you are looking for a needle in a haystack, you need to shrink the size of the haystack; in security terms, that means removing legitimate travelers and cargo from the queue while focusing on the areas of highest risk.

A perimeter approach to security would allow us to manage risks at the Canada-U.S. border without militarising it. It would focus on intercepting terrorists and their weapons long before they reach our shores. Our efforts to counter an international network of terrorist cells must involve cooperation with other nations to eliminate the

threats where they exist and not wait until they attempt to enter our country. This does not mean that security along the forty-ninth parallel will disappear, only that it will become more strategic, more focused and more efficient.

In 2008 and again in 2009 the Canadian Chamber of Commerce and the U.S. Chamber of Commerce partnered with over 40 business associations on both sides of the border to launch a report on improving border efficiency. The recommendations put forth in the 2009 report: *Finding the Balance: Shared Border of the Future* embrace the post 9/11 security environment and are designed to reduce border costs while strengthening security. These recommendations recognised that, while new infrastructure is urgently needed, there are still some things we can do to make our current facilities function better.

First, we should focus the limited resources of border agents where they are most needed—on unknown cargo and travel. Both governments have recognized this need and there has been good progress improving trusted shipper and trusted traveller programs.

Programs such as Free and Secure Trade (FAST), NEXUS, Customs Self-Assessment (CSA), Customs-Trade Partnership against Terrorism (C-TPAT) and Partners in Protection are all excellent ways to reduce border congestion.

The Canadian Chamber of Commerce is a strong advocate of such voluntary programs. Unfortunately, businesses on both sides of the border are finding that the benefits from trusted trader and traveller programs do not outweigh the costs. Both governments can work together to find ways to increase the benefits for participation in trusted shipper and traveller programs—including participation by other government departments.

A good example of how this can be done is the experiments in expedited security processing for NEXUS cardholders at certain Canadian airports. It is worth noting that the NEXUS card is being used for domestic travel and not just for Canada-U.S. trips. That's not the primary purpose of the cards, but it conveys added benefits that will encourage more people to enrol in the program.

Second, both governments need to be prepared for an unexpected closure of the border. There are several factors that could temporarily shut down border operations, including pandemics, terrorist attacks or natural disasters. Such closures would have a major impact on North American supply chains and on economic stability.

Both governments have recognized the importance of keeping the border functional during an emergency. In 2009 the Canadian government released its *Plan for the Movement of People and Goods During and Following an Emergency*. This contingency plan is designed to ensure that priority people and goods can cross the border during an emergency. While it is a welcome initiative, CBSA must continue to work with CBP in the development of a joint contingency plan that builds upon the 2009 framework.

Third, we need to address the structural constraints at the border that can lead to unpredictable or onerous wait times. Insufficient border infrastructure, poor training of customs officials, inadequate staffing, lack of modern technology, insufficient information about updates to

security and regulatory requirements, and redundant processes and procedures all add to border wait times.

The Canadian and U.S. governments should collaborate in developing accurate staffing models for border services that reflect and respond to demand. This includes working with other government departments with border mandates to develop a single window, examining a range of preclearance options and offering support services 24/7 at major border crossings.

In terms of border infrastructure, one of the greatest challenges we face is that the most important crossings between Canada and the United States are at geographic choke points. They are above or below bodies of water. It is not as easy as slapping down several more lanes. Our two governments have done a great deal to improve throughput in these bottlenecks, but more can be done. For example, the age of our current facilities is a serious problem. The key border infrastructure dates back to our grandparents' day and there is a dire need to expand and modernize it. There is no doubt that this is a matter of national security, and it is hard to think of any other two

countries anywhere in the world that would have taken so long to modernise infrastructure that is so vital for the economic and physical wellbeing of their citizens.

It is important to keep in mind that in today's reality, borders exist wherever sovereignties intersect. Our enemy fights according to lethally unconventional rules, which means that no country can simply draw a line around its physical boundaries and consider itself secure. For instance, physical fortification of the border has little meaning if our systems remain vulnerable to cyberattacks. The internet has become an invaluable tool of our day to day lives—we live, work and play online. Yet cyberspace has created a new security dimension—one that is constantly evolving to unveil new vulnerabilities and new threats. Our reliance on cyberspace has made us susceptible to those who would exploit this dependence for their own gain.

The internet is an ideal location for criminals and terrorists where they do not have to worry about passports or visas. As Wikileaks has shown us, it can also offer them access to sensitive personal, economic or military data. Cyberspace opens a door into our homes,

our businesses and our government offices. We must ensure that we can protect ourselves from innovative and determined cyber criminals. Canadian citizens and Canadian businesses are increasingly concerned with cybersecurity. President Obama has estimated that over \$1 trillion USD was lost thanks to cybercrime in 2008. Yet, despite the extent of the problem, progress on the creation of a global legal framework to combat cybercrime has been shockingly slow.

There is also growing concern about the threat of cyber terrorism. The use of computer systems for the perpetration of terrorist attacks is undeniable. Terrorist organizations have been using the web to spread propaganda, recruit and fundraise. They have also recognized the potential to undermine North American security through cyber attacks. While an apocalyptic attack on our cyber systems appears unlikely in the near term, persistent hackers continue to put pressure on even the most secure systems.

This issue is in the news again this week. The New York Times reported that the leaked diplomatic cables claim the Chinese politburo

has directed cyberattacks on Google, on government computers and on other private sector companies. Similarly, the press has reported that Western agencies have planted computer worms in the centrifuges used in Iranian nuclear reactors. There is no reason to believe that key pieces of our own critical infrastructure may not be the target of similar attacks.

The Canadian government recently announced its commitment to protect our cyber security in *Canada's Cyber Security Strategy*, which recognizes the need for greater international cooperation. Canada should continue to build on its cyber strategy including through the identification of priorities areas and by strengthening the institutional capacity to protect vulnerable networks. Given our shared security risks and the integration of many critical infrastructure areas, it only makes sense for Canada and the U.S. to collaborate on the protection of our digital assets.

Although terrorism remains a priority when considering the protection of critical infrastructure, it is by no means the only threat. We are only beginning to grasp what effects climate change may bring. Warmer,

dryer summers and stronger more intense storms are all possible challenges that we may face. We have already witnessed the massive damage that can be caused by extreme weather. Hurricane Katrina physically devastated New Orleans and disrupted power and communications in many surrounding states. Residents in the affected regions could not withdraw cash from ATMs since the systems were down, while many branch locations had been destroyed. Roadways that were flooded or clogged with debris complicated rescue efforts. Similar problems were experienced in the UK during the 2007 floods where some areas received a month's worth of rain in 24 hours.

Canada has thus far been lucky when it comes to natural disasters. However, we all remember the Ice Storm of 1998. A major disruption to critical services on a similar scale is not a matter of "if" but of "when."

We must ensure that the systems responsible for public utilities are adequately protected from both natural and man-made disruptions. For example, the energy sector is vital to North America's economic

stability. Since 1980, Canada's production of energy has almost doubled so that today, the Canadian energy sector accounts for \$70 billion worth of our GDP. We are the largest producer of uranium for fuel, the third largest producer of natural gas and hydro electricity, the seventh largest producer of crude oil and nuclear energy, and the eighth largest producer of petroleum products. We are the largest single supplier of energy to the US. Our energy systems are closely interlinked through a network of pipelines, commercial operations and grids. Unfortunately, North America's energy integration makes it particularly vulnerable to disruption.

The consequences of a wide-scale interruption to energy services would be disastrous. Take, for example, a terrorist attack against one of the main sources of energy production, such as a hydroelectric dam. Such an attack would disrupt power generation, which would in turn affect various transportation modes, such as rail and air. This would not only disrupt commercial transactions, but would cause serious environmental damage as well. We have already witnessed the serious economic and environmental effects caused by this summer's disaster in the Gulf of Mexico.

When developing strategies for the protection of critical infrastructure, there are several important facts to bear in mind. First, many critical infrastructure sectors are privately owned and operated. The majority of public and private owners have already established their own contingency plans and reliability standards. Any new regulations or legislation adopted by the government must not be so onerous as to hinder future investments in critical infrastructure. Additionally, the rapid pace of technological advance in many critical infrastructure areas can make it difficult for the government to keep up with the rate of change. That is why government must work with the private sector in developing critical infrastructure protection strategies.

Second, the first responders in emergency situations are most often the owners and operators of critical infrastructure or the municipalities or jurisdictions in which the disruptions occur. Minimizing the damages from these disruptions is vital. Ensuring the rapid resumption of services depends upon the strength of partnerships at the local, regional and national level and the timeliness and accuracy of communications. The communication failure following this

summer's earthquake demonstrates the importance of information accessibility during a crisis. In this instance, not only were some Canadian websites overloaded by traffic volumes, but it was clear that overly centralized information control mechanisms are vulnerable to failure in crisis situations. We must learn from these experiences and improve our systems so we are better positioned for rapid response in the future.

The cross-jurisdictional nature of critical infrastructure protection makes communication and cooperation among relevant stakeholders indispensable. The federal government has an important role to play in coordinating the administrative, regulatory and enforcement efforts among the private sector, local and provincial and or state authorities as well as with other government departments. It can also organize table-top exercises and simulations to develop a better understanding of the functionality of processes and procedures during a crisis situation.

Third, businesses must be assured that any information that they provide will be respected and held confidential. Many firms are wary

of sharing information with their competitors, despite recognizing the need for collaboration. Some opportunities for collaboration include the promotion of best practices, collaborative development of standards, the identification of threats, cost sharing and raising awareness.

Finally, system upgrades to improve resiliency can be expensive—both to build and to maintain. It would be impossible to protect all systems completely. There is a need to prioritize vulnerabilities and conduct risk assessments to understand where progress is most needed.

In all of these areas, as in all of the other measures we take to protect our citizens from threats, Canada and the U.S. need to work with each other to find common solutions. The process may generate frustrations on both sides of the border, and may not always develop in the way that we envision. When both the safety and the standard of living of our citizens in each of our countries hang in the balance, the stakes are too high for us not to work together. It is vital that we

increase our efforts to develop, implement and test our strategies to protect our critical infrastructure and our citizens.

– 30 –