Remarks by the Director of the Intelligence Staff
Lieutenant General Ronald L. Burgess, Jr., USA

Canadian Association for Intelligence and Security Studies
2008 International Conference

Crowne Plaza Hotel
Ottawa, Canada

November 1, 2008

AS PREPARED FOR DELIVERY

Good morning – and thanks for that introduction. It's great to be here today. It's always nice to get out of Washington, but especially nice during election season.

On the flight over here, I had the opportunity to read through last year's CASIS Conference Report – I wanted to get a sense of the overarching issues and themes that concerned the participants roughly one year ago. One thing that I found especially interesting: many of the conference speakers identified cooperation and collaboration as more important than ever in security and intelligence, and were calling for more holistic approaches than in the past. I couldn't agree more, and as Director of the Intelligence Staff, I have gone around the U.S. Intelligence Community talking about the DNI's goals for transforming the way that we operate – goals that could be summed up in one word: *collaborate*.

Now, it's certainly hard to be against collaboration, but then I heard a joke that proved me wrong.

Three castaways – John, Mike, and Jim – are washed ashore on a deserted island, cold and wet, with no food, water, or shelter. They conclude very quickly that they will have to work together to survive, and they set out to do just that.

Then one day, as they are strolling down the beach, they come across a tarnished, old brass lamp half-buried in the sand. We all know what to do with an old, tarnished brass lamp, and they do as well – they immediately rub the lamp, and lo and behold, out pops a Genie, who says, "Thank you for releasing me from my prison. Out of gratitude, I shall grant you three wishes…one wish apiece."

Mike thinks a bit and then says, "I am just sick and tired of eating fish and coconuts, so I wish I was in Paris (or maybe it should be Montreal?), at the finest French restaurant, with a gourmet meal before me." And POOF! Mike is gone.

Jim goes next. He thinks for a bit and says, "French restaurants and gourmet meals are fine, but I am sick of all this heat, so I wish I was sitting under a shade tree, next to a cool mountain stream in the high Rockies." And POOF! Jim is gone.

That leaves John. He thinks, and thinks, and thinks some more. He is clearly struggling with his choice, especially since he knows he only has one chance. Frustrated, he turns to the Genie and says, "You know, with gourmet meals and cool mountain streams and all the other possibilities, I just cannot seem to decide. I sure wish Mike and Jim were here to help me figure this out." And suddenly, he hears POOF! POOF!

And there you have it, the downside of collaboration.

In all seriousness, however, collaboration could not be more critical at this juncture in time. We live in a dynamic world in which the pace, scope, and complexity of change are increasing. Increased global connectivity, interdependence and complexity create a less predictable future. Globalization—while it has certainly opened up avenues for growth and prosperity around the world—has also complicated persistent threats and has generated emerging missions, such as cyber, energy, and infectious disease. In addition, changing demographics, population stresses, and resource scarcities have the potential to create economic and political instability worldwide, which will create an entirely new set of national security challenges for the U.S., Canada, and other Western nations. To succeed in this new world, we must be able to rapidly and accurately anticipate and adapt to complex challenges. And we must be able to out-maneuver our adversaries—not just out-muscle them.

This makes intelligence more critical than ever.

Our mission in the U.S. Intelligence Community is to create decision advantage through a globally-networked and integrated intelligence enterprise. Decision advantage means that we improve our ability to make decisions at every level—from our top leaders to the soldier on the front lines—while denying our adversaries the same advantage.

An important aspect of decision advantage lies in addressing critical national security missions and preparing our decision-makers for strategic surprises—that is, those forces or issues that lie outside the current agenda but may emerge to challenge our intended outcomes. In an increasingly interconnected and complex world, the Intelligence Enterprise must enhance its capabilities to evaluate the entire spectrum of global threats and risks affecting our national security.

A few months ago, in July, DNI McConnell released Vision 2015, which discusses the key components necessary to achieve a globally networked and integrated intelligence enterprise. Now, if you're really interested in the nuts and bolts, you can go to our website (www.dni.gov) and read through the entire document. But let me go through some of the key elements:

- Against the backdrop of an expanding customer landscape, we need to transition to a more customer-driven intelligence model. By 2015, the Intelligence Enterprise will be expected to provide more details about more issues to more customers, who increasingly

will demand more tailored operational and analytic support. The key decision makers of the future will include individuals who will demand instant information, access to seamless technological expertise, and greater cross-agency collaboration in the development of products and information.

- We are also moving toward more mission-focused operations—a concept of operations that transcends the current agency-centric model towards a more mission-based configuration that is agile, synchronizes collection, and connects dispersed and divergent expertise to collaborate on hard problems. That's why we established the NIC-C (the National Intelligence Coordination Center) back in October 2007 for all-source intelligence collection coordination and tasking deconfliction. The NIC-C provides a mechanism to strategically manage and direct collection across defense, foreign, and domestic realms, and will ensure that we are able to leverage existing capabilities all across the U.S. Government.

- We want to build a net-centric information enterprise – a common information infrastructure that provides seamless access to intelligence information, services, and tools across multiple agencies and databases. It's not always easy to break down some of the longstanding policy and technological barriers in place, but we're making excellent progress. For example, we've taken some best practices from the private sector and have implemented what we like to call "Intellipedia" – an internal Web destination where analysts across the CIA, FBI, DIA and other intelligence agencies can swap what they know with one another. The result is a collective intelligence that goes beyond the "smarts" of any one agency. We're also working on something called A-Space—modeled after the highly successful social networking sites that young people use, such as Facebook and My-Space—which allows analysts to post their research, so that others can read and comment on the information, and share videos, audio, and documents. It essentially allows for a virtual dialogue in real-time among a much larger group of users. Intellipedia and A-Space represent a new way of thinking and a fresh approach for the U.S. Intelligence Community – we're learning from commercial and open-source software, as well as adopting means of communication already popular among a new generation of analysts, and applying new work methods and processes to the business of intelligence.

- Finally, we are moving to a more integrated enterprise. Collaboration does not just "happen." It needs a strong institutional foundation that integrates the vital components of the Intelligence Enterprise – policy, people, processes, infrastructure, and technology – to remove longstanding barriers to collaboration.

Sans Frontiers

Security, Intelligence Law Enforcement and Defense *Sans Frontiers*, the theme the Canadian Association for Security and Intelligence Studies (CASIS) chose for this year's conference, correlates closely with what we see as essential to achieve decision advantage – transcendence of both geographic and organizational boundaries.

We know that the challenges we face are increasingly without borders – persistent threats such as cyber attacks, threats to global commerce, terrorism, and transnational crime.

In its report on "Mapping the Global Future," our National Intelligence Council highlighted globalization—the growing interconnectedness reflected in the expanded flows of information, technology, capital, natural resources, services and people throughout the world. The report referred to globalization an "overarching 'megatrend,' a force so ubiquitous that it will substantially shape all the other major trends in the world of 2020."

Our infrastructure of global networks of information, finance, commerce, transportation, and people increasingly is being targeted for exploitation, and potentially for disruption or destruction, by a growing array of state and non-state actors.

In this new environment, geographic borders and jurisdictional boundaries are blurring; traditional distinctions between intelligence and operations, strategic and tactical, and foreign and domestic are fading; the definitions of intelligence and information, analysts and collectors, customers and producers, private and public, and competitors and allies are changing. Even distinguishing between intelligence and non-intelligence issues may prove to be a major challenge.

Strategic Partnerships

In response to these challenges, Vision 2015 spells out the need to develop strategic partnerships without regard to borders. This includes developing enduring partnerships with segments of our societies that have not traditionally been thought of as intelligence resources, and even deeper relationships with our closest Allies. These partnerships encompass our traditional international allies, but must also extend to relationships with academia, industry, law enforcement and other organizations not traditionally involved in intelligence, to reap the benefit of their abilities and expertise.

Of course, the U.S. & Canada—with our shared border and common interests—have cultivated and maintained an outstanding security arrangement for more than a half-century. As a result, our countries have developed a strong and multifaceted intelligence relationship.

Take, for example, the fact that Canada and the U.S. share the world's longest border. Both our governments are committed to monitoring and securing this border from attempts by terrorists to enter the U.S. from Canada and vice versa. Building on an already outstanding relationship, the U.S. will continue to seek ever greater cooperation with the Royal Canadian Mounted Police (RCMP) and broaden and strengthen intelligence relations with other Canadian agencies involved in homeland security, particularly on terrorist tracking efforts.

The Canadian law enforcement community also works extensively and effectively with the U.S. Department of Homeland Security on issues of shared concern, such as criminality and border security, working jointly toward the goal of "collective North American security."

Forging a law enforcement/intelligence nexus could provide new opportunities and venues for collaborative work on gaps and targets, and U.S./Canadian cooperation in the intelligence arena is certainly a relationship that we want to continue, and improve.

In the future, for example, we hope that Canada and the U.S. will collaborate more closely on transnational crime and other threats that more directly affect Canadian citizens, to bring about a jointly-secured North American continent. Alien smuggling, human trafficking, and drug smuggling are other areas in which we may collaborate more fully.

And the US looks forward to supporting Canada on security preparations for the 2010 Winter Olympics, which have already begun in earnest. It will give both our nations a unique opportunity to develop and test security capabilities jointly, to ensure the safety of our international athletes and attendees.

Partnering Across Organizational Boundaries

Partnership and collaboration are not limited to our international allies, however. Within the U.S. Intelligence Community itself, we are also working to break down stove-pipes and partner across organizational boundaries, where the model of individual agencies controlling information collected by specific disciplines (IMINT, SIGINT, etc.) no longer works as it did during the Cold War.

Now, this is not to imply that breaking down these barriers—be they cultural, technological, or legal—is easy. It's not. We simply cannot get around the fundamental reality that change is hard – and unfortunately, change is often slow. And in fact, very often, a large bureaucracy will choose failure over change. As we all know, however, in our business – failure is not an option. The stakes are just too high.

So we are committed to breaking down these boundaries within our 16-agency Intelligence Community, but just as important, we're committed to working with our international counterparts to assist in your efforts to streamline your own intelligence enterprise. We would welcome the opportunity to sit down with our Canadian counterparts and share some of our own "lessons learned" in breaking down barriers within our own intelligence community.

For example, one of the simplest and most effective changes undertaken in the U.S. is a standardized badge that will enable access to each other's intelligence agencies. Seems like a no-brainer, right? Well, it actually turned out to be one of the first steps to having our personnel view themselves as part of an integrated intelligence enterprise. In addition, it reduced the resources we had to invest in passing clearances and issuing visitor badges whenever individuals from different intelligence agencies would meet with one another.

To deepen and further promote that cultural integration, the U.S. Intelligence Community has implemented a program called Joint Duty. The inherent cross-cutting challenges facing our Community today require professionals and senior leaders with an understanding and awareness of the entire IC, as well as established relationships beyond one single agency. The joint duty program provides rotational career opportunities for civilian IC professionals, enabling

intelligence officers to gain an enterprise-wide perspective, cultivate cross-organizational networks, and share information with their counterparts more easily. Ultimately, we hope that joint duty will result in a wide cadre of intelligence officers with a keen appreciation for another agency's culture, body of expertise, and business practices. We hope joint duty will allow our intelligence professionals to leverage the unique skills and expertise from across the IC and bring them to bear against complex threats.

Joint Duty transformed our military into a unified fighting force, and we believe it can do the same for the U.S. Intelligence Community. The program is not just about working in another agency; it is about learning how to collaborate, integrate, and lead across agencies as well as operate with the speed and agility needed to defeat 21st century adversaries.

Finally, we must figure out a way to meet these challenges at the same time that the Community itself is evolving. As baby boomers retire in ever increasing numbers, U.S. intelligence organizations are becoming staffed by a majority of employees with less than 5 years experience in intelligence. This presents a whole host of challenges, of course, in that we need to find a way to replace large numbers of retirees, who take with them an immeasurable wealth of knowledge and deep expertise. It does, however, present opportunities to evolve as a Community. The next generation entering our workforce has grown up on the internet; they have an integral understanding of a virtual world without borders and they are demanding that intelligence adapt to their more integrated, dynamic culture, one that is comfortable sharing information. One of our highest priorities must be to transfer that agility, adaptability and culture of sharing to the intelligence workplace.

Reaching Out to Non-Traditional Resources

Now, I've spoken a bit about how we need to develop partnerships internally—that is, within our own Community—as well as strengthen our existing ties with our Canadian intelligence counterparts. But we also need to develop *new* partnerships; this means reaching out to non-traditional resources that might include government organizations outside the intelligence community or beyond the federal level, such as:

- state & local law enforcement;
- the academic community; and
- the private sector – particularly those industry elements that now control so much of our critical infrastructure.

Our interdependence among defense and national security contractors when it comes to critical infrastructure and defense information systems means that we need a fundamental re-thinking of our government's traditional relationship with the private sector. A high percentage of our critical information infrastructure is privately owned, and industry need to know what government knows about our adversaries' targets and, to the extent we understand them, their methods of operation. When it comes to cyber security, government and the private sector need to recognize that an individual vulnerability is a common weakness.

In the analytic arena, we're increasingly reaching out to outside expertise. For example, for the past two years we've run SHARP—the Summer Hard Problem Program. This annual, month-long, intensive study program investigates timely and difficult intelligence topics by engaging a diverse set of external experts from the private sector to work alongside internal government personnel in a secluded, classified setting.

The goal of this intensive four-week program is to engage external (non-government) experts on a problem of critical interest to the IC and thereby enhance the IC's ability to collect, analyze, and integrate intelligence relevant to national security threats. By eliciting the perspective of external experts and fostering collaboration with government officials on a particular intelligence issue, we can identify novel approaches that offer innovative solutions to analysis and collection challenges. Further, the relationships developed at SHARP form the foundation for ongoing professional collaboration and a continual exchange of insights, which are so vital to national security.

Accordingly, our strategic partnerships must continue to include organizations such as CASIS, which can offer a wellspring of new ideas to meet persistent threats. CASIS provides an ideal venue to strengthen interdisciplinary approaches to addressing security and intelligence issues—to train the next generation of intelligence professionals, to provide new perspectives to senior leaders and government officials, and to break down cultural barriers between traditional intelligence partners and non traditional ones.

Canada faces many of the same issues that we in the United States face, and we must continue to work together—not only to identify and address the critical intelligence issues of our time—but to jointly develop solutions to remove the remaining barriers that inhibit collaboration, intelligence sharing, and problem-solving and keep us all from achieving decision advantage. *Sans Frontiers* – that's got to be our rallying cry.

I challenge CASIS to bring its considerable expertise to help chart a new way forward for overcoming our adversaries and making optimum use of the intelligence discipline for the collective benefit of our two great nations.

Thank you for this opportunity to be with you all today and I welcome any questions or comments you might have.