Submission to the Digital Economy Strategy Consultation

Canadian Internet Registration Authority

cira | .ca Canadians Connected

July 2010

Report Title: Submission to the Digital Economy Strategy Consultation

Date Published: July 2010

The Canadian Internet Registration Authority (CIRA) is the organization that manages the .CA domain space on behalf of all Canadians.

This report should be cited as follows:

Canadian Internet Registration Authority. (2010). *Submission to the Digital Economy Strategy Consultation*. Ottawa: Author.

For queries or copyright requests, please contact:

Canadian Internet Registration Authority
350 Sparks Street, Suite 306
Ottawa, ON K1R 7S8
Tel: (613) 237-5335

E-mail: info@cira.ca
Website: www.cira.ca

Table of Contents

About the Canadian Internet Registration Authority (CIRA)

The Canadian Internet Registration Authority (CIRA) is the organization that manages the .CA domain space, Canada's space in the Internet's global Domain Name System (DNS), on behalf of all Canadians. The Government of Canada has formally recognized and designated CIRA as the administrator of the .CA domain space. CIRA takes an active interest in policies that support Canada's Internet community and is an active participant in international Internet governance fora.

The DNS is vital to the Internet but generally invisible to users. It is a widely distributed and robust structure that maps domain names, like Canada.ca, to the strings of numbers that make up Internet Protocol (IP) addresses – and vice versa. CIRA is responsible for operating the registry database and the authoritative name server network for the .CA Internet country code Top-Level Domain (ccTLD).

.CA is a public resource for all Canadians. Started by volunteers at the University of British Columbia, the .CA domain was officially transferred to CIRA in December 2000. .CA has since grown rapidly to become one of world's largest ccTLDs with nearly 1.5 million domain names. CIRA is recognized as a leader among DNS registries and a model for others.

CIRA is a not-for-profit corporation governed by a 15-member Board of Directors, consisting of elected and appointed members (one ex-officio member is from Industry Canada). Directors are elected annually by CIRA members in an online process. Membership in CIRA is free, and open to anyone who holds a .CA domain name.

CIRA's global network of more than 50 nodes ensures timely access to .CA domains worldwide. Its relationship with the Internet Corporation for Assigned Names and Numbers (ICANN), which manages the DNS globally, ensures world-wide connectivity for .CA domain names. CIRA has contractual relations with all organizations that register .CA domain names (Registrars) and with all individuals and organizations that hold .CA domain names (Registrants). This includes the Government of Canada. Through its management of the .CA domain, CIRA provides a critical part of Canada's digital economy infrastructure, enabling global e-commerce with a Canadian presence, 24 hours a day, seven days a week.

The .CA Top-Level Domain

In 2009, the .CA domain had a 27 per cent market share in Canada, second to .COM. However, the .CA top level domain has enjoyed considerable growth in spite of the recent global economic downturn. Between 2007 and 2009, .CA registrations grew by 16 per cent, significantly higher than the annual global growth rate of generic Top-Level Domains (gTLDs) at six per cent.

CIRA views the .CA domain space as a marker of Canada's online identity, and has conducted sufficient research to substantiate this opinion.

In a 2008 survey of 1,033 adult Canadian Internet users, the primary reason given for choosing to register a .CA domain name (60 per cent) was that it is Canadian. In the same study, 95 per cent of respondents ascribed, "used by Canadian organizations and companies," as the best descriptor of .CA domain names. The Canadian Presence Requirements for .CA domain names were considered important by 93 per cent of the survey respondents.

In the same survey, 73 per cent of respondents stated that, "trustworthy and honest," was the best descriptor of .CA domain names. In comparison, only 27 per cent of respondents thought trustworthiness was the best descriptor of .COM domain names.

Canadian Internet users were also asked to identify their preferred domain name for banking and shopping, .CA or .COM. The responses were overwhelmingly in favour of .CA, with 78 per cent of respondents preferring .CA domain names for banking and 60 per cent of respondents preferring .COM domain names for online shopping. A 2007 survey by Statistics Canada showed that Canadians placed $12.8 billion worth of orders online, of which $7.1 billion was spent with Canadian companies.

Interestingly, in the same study, 85 per cent agreed that Canadian businesses and organizations should use .CA for their websites.

Clearly, Canadians view the .CA domain space as safe, secure and reliable, and believe that .CA is integral to the identification of secure online e-commerce websites.

For Canada to take a leading role in the online economy, Canadian consumers must have trust in their online transactions.

Recommendation 1: The .CA domain name extension is a visible marker of online security, and the Canadian government should champion use of it by:

- Requiring all websites developed or contracted by the government use the .CA domain name extension.
- Encouraging partner and arms length organizations to use the .CA domain name extension.
- Encouraging use of the .CA domain name extension by Canadians through its related communications materials.

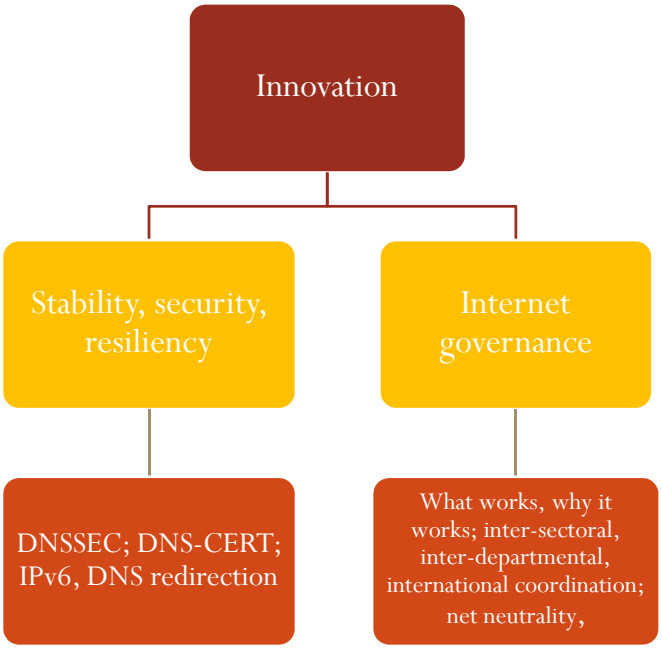
SUMMARY OF CIRA'S SUBMISSION

CIRA welcomes the opportunity to participate in this Industry Canada (IC) consultation. As the steward of Canada's Internet top level domain, CIRA's primary concern in this consultation is the Internet-driven value chain of creativity, innovation, productivity, and competitiveness. *This is the value chain of the digital economy*.

The Internet became this value chain's central driver in the 1990s and it will continue to be the key driver well into the 21st century. It has been called a "digital tornado" and it is transforming wealth creation. Its capacity for "creative destruction" is legendary. Its reach and impact are both global and local. Digital technology, openness and global access are the characteristics of the Internet that drive this value chain. But these same characteristics also enable on-line threats that undermine security and trust. As well, the Internet's unprecedented growth has put great strain on the underlying legacy telecommunications infrastructure on which it runs. At this juncture, CIRA believes that concerns about network security, network capacity (bandwidth) and price are the single greatest barriers to the Internet-driven value chain in Canada.

Accordingly, the two-part theme of this submission is that, for Canada to take full advantage of the digital economy value chain: ***1) the characteristics of the Internet that have underpinned its success need to be safeguarded and strengthened; while, 2) measures that foster greater security and reliability must be implemented to enable increased trust and confidence in Internet transactions.*** *In short, from CIRA's perspective the best digital economy strategy for Canada is a policy framework that provides a climate for creativity, innovation, productivity and competitiveness.*

CIRA's submission responds primarily to questions raised by the government's consultation paper about innovation. To the extent that issues raised in other sections of the consultation paper relate to this central theme, CIRA will comment briefly. From CIRA's perspective, issues that underpin this value chain in the context of the Internet are illustrated in the graphic below, which also serves as an outline for this submission:

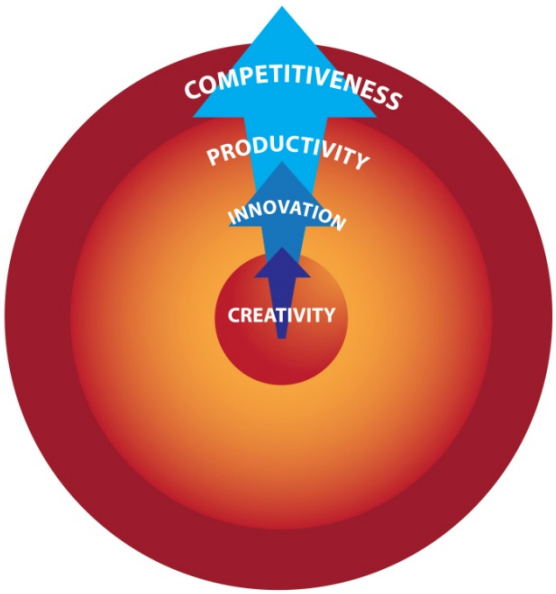


How the Internet Drives the Digital Economy Value Chain

The Internet's tremendous capacity for enabling economic growth has been well documented. From a technical perspective it is the combination of digital technologies, open standards, open access, and unmediated global and local reach that unleashed an explosion of creativity, freedom of communication, bottom-up innovation and creative destruction. These characteristics accomplish the following:

- Tear down barriers to communication.
- Accelerate transactions and overcome distances.
- Facilitate collaboration among users around the world.
- Expose local ideas, issues and developments to global audiences.
- Drive down costs of production, communication and delivery.
- Open up global markets to local products and services.
- Turn niche interests and markets into global communities.

The Digital Economy Value Chain



All of this happens in real-time – in Internet time. *So the Internet stimulates human **creativity** with new technologies, outlets and opportunities; this leads to **innovation** in products, services and processes; which improves **productivity** for individuals and businesses; and boosts their **competitiveness** in the global digital economy.*

These characteristics distinguish the Internet from the legacy telecommunications and broadcasting networks in fundamental ways. The Internet was designed to be user-centric, enabling direct, unmediated communication and transactions among end-users. The legacy networks were network-operator-centric: either tightly controlled and managed (telecommunications) or one-way only (broadcasting).

Neither of the legacy network designs was capable of enabling the widespread user-generated creativity and innovation that the Internet has delivered. Yet they form the underlying infrastructure on which the Internet runs. The relationship has never been easy. On one hand the Internet drives demand for network capacity and reach, and ever-more investment in an already capital intensive industry. On the other hand, while digital technologies and open standards lower costs, they also enable new competition for legacy network operators, push down prices and change revenue streams.

The user-centric Internet is indifferent to all traditional industrial sectors or fields of endeavour. No one could have foreseen the great success of on-line services such as VoIP, Google, e-Bay, YouTube, Facebook, Twitter, and Amazon. No one could have foreseen the evolution of the music distribution industry. No one could have foreseen the rise of a dynamic and globally competitive on-line gaming industry in Canada. No one can foresee today the impact of millions of daily on-line transactions tomorrow on the direction of future growth in one economic sector or another.

These characteristics inform CIRA's responses, presented in the following sections of this submission, to the questions posed in the consultation paper.

A Climate for Creativity, Innovation, Productivity, and Competitiveness

Focal Points for a Digital Economy Strategy

- Industry Canada question: *Should Canada focus on increasing innovation in some key sectors or focus on providing the foundation for innovation across the economy?*

From CIRA's perspective, the answer is clear: in the digital economy, government should not try to pick winners with taxpayers' money. The digital economy value chain is simply too fluid, open, subject to global market forces, and unpredictable. Let individual Canadians and businesses determine the most efficient and effective opportunities, building on Canada's evolving competitive advantages and opportunities.

> **Recommendation 2:** The Government of Canada's digital economy strategy should focus on providing a foundation that enables innovation across the whole economy, by updating laws and regulations to ensure confidence and trust in on-line transactions, by removing barriers to the digital economy value chain wherever it can, and where demonstrably required, by providing targeted incentives that foster creativity and innovation, in particular for research and development.

- Industry Canada question: *Which conditions best incent and promote adoption of ICT by Canadian businesses and public sectors?*

Given the nature of the digital economy value chain, delayed adoption of information and communications technologies (ICTs) is almost certainly a barrier to success. It is outside CIRA's area of expertise to suggest specific measures or conditions that may stimulate accelerated adoption. However, CIRA believes that government can play an important role in identifying and removing barriers.

> **Recommendation 3:** The Government of Canada undertake research to assess whether specific market conditions in Canada impede adoption and/or whether aspects of Canada's fiscal and tax framework can be modified to spur adoption of Information and Communications Technology (ICT) by Canadian businesses and public sectors.

As for the public sector, governments are among Canada's largest employers and users of the Internet, and government services touch Canadians daily. Governments are well positioned to take a leadership role by becoming informed and demanding users of ICTs. The resources and coordination required to pursue this role would almost certainly be off-set by the benefits of removing technological barriers to service delivery in the public service (improving both productivity and job satisfaction) and economy-wide spin-off benefits from driving accelerated private sector adoption. As discussed in the following section of this submission, one area where governments could make a significant difference is by itself adopting, and promoting broader Canadian adoption of, Internet Protocol version 6 (IPv6).

> **Recommendation 4:** Governments in Canada should develop strategies to become more informed and demanding users of ICTs and the Internet.

Internet Governance, and Stability, Security, Resiliency of the Internet

To facilitate discussion, CIRA's responses to the following three Industry Canada questions are grouped under two interrelated sub-sections in this part of our submission: a) Internet Governance; and b) Stability, Security and Resiliency.

- Industry Canada question: *What would a successful digital strategy look like for your firm or sector? What are the barriers to implementation?*
- Industry Canada question: *Once anti-spam legislation, and privacy and copyright amendments are in place, are there new legislative or policy changes needed to deal with emerging technologies and new threats to the online marketplace?*
- Industry Canada question: *How can Canada use its regulatory and policy regime to promote Canada as a favourable environment for e-commerce?*

Internet Governance

Given the Internet's open, decentralized and transborder nature, the term "Internet governance" may seem like an oxymoron to many. However, from its inception, the Internet's openness, adaptability and resiliency have evolved through bottom-up, consensus-based decision-making. The framework for this evolution is a loose collection of formal and informal global, multi-stakeholder, non-governmental organizations in which governments, the private sector, academia, and a range of public interest groups collectively known as "civil society", all participate as equals. This is "Internet governance". It has proven to be remarkably effective and efficient in ensuring a stable, robust and resilient Internet. Moreover, in countries where the Internet has flourished, governments have generally taken a hands-off or light-touch approach domestically. *This approach to Internet governance is central to safeguarding and preserving the characteristics of the Internet that have underpinned its success.*

Global Framework

Some elements of the global Internet governance framework have existed for many years while others are relatively new. At the core are two key technical functions: the development of technical standards or "protocols", and the management of the global DNS. Around these core functions have grown a range of issues and organizations.

The Internet started as a U.S. government financed military and research internetworking project. As the project evolved into the public, commercial Internet, the U.S. government decided to devolve responsibility for the core technical functions out of government. Internet standards were already being developed by the Internet Engineering Task Force (IETF), an informal group of engineers from government, academia and business. But the DNS function was operated under contract to the U.S. government. By the mid 1990s, the Internet was already global and included many ccTLDs, like .CA, serving other countries. The devolution of the DNS function was done after a vast international consultation. This led to the creation, in 1998, of the not-for-profit ICANN, to manage the DNS, including the central Internet Assigned Numbers Authority (IANA) registry or "root server".

Some governments opposed this approach. They wanted the DNS to be managed by an intergovernmental treaty organization, the International Telecommunication Union (ITU) of the United Nations, which coordinates global use of radio frequencies and telecom standards. The Government of Canada, however, was and has continued to be a strong supporter of the approach adopted by the U.S. Given the Internet's fast-paced, bottom up evolution, Canada and the U.S. have taken the view that a private sector led not-for-profit organization is better suited than

governments to manage the Internet's core technical functions. The devolution is nearing completion, as the U.S. government gradually extricates itself from residual contractual arrangements with ICANN.

However, given the Internet's global reach, governments saw policy issues arising out of the operations of these technical functions as trans-border e-commerce and communications grew in importance. International business also had a vested interest. So did civil society public interest groups. Issues included, for example, how to ensure a competitive market with monopoly DNS registries like the .COM, .NET and ccTLDs; the relationship of ccTLDs to the governments of the territories they serve; protection of intellectual property as corporate names became Internet domains; and, the evolution of the DNS to fully accommodate scripts for languages other than English.

In response, the global framework for Internet governance has evolved to accommodate broad multistakeholder participation. As noted above, this framework is a loose, interconnected collection of formal and informal global non-governmental bodies in which governments participate as equals with the private sector, academia and civil society. These organizations include, but are not limited to the following:

- **The Internet Engineering Task Force** (IETF) is the principal body engaged in the development of new Internet standards. Formed in 1986, the IETF brings together engineers from private sector, academia and government. The IETF's official documents are the outcomes of "requests for comment" and therefore known as RFCs. Though non-binding, they are almost universally adopted and available free of charge. Find more on the IETF at www.ietf.org.
- **The Internet Corporation for Assigned Names and Numbers** (ICANN) is a California-based not-for-profit that coordinates the allocation and assignment of the Internet's unique name and number identifiers, and policies related to these technical functions. There are three supporting organisations each for IP addresses, domain names and country code top-level domains. As well, there are four advisory committees each for governments and international treaty organizations, root server operators, Internet security, and average Internet users. A Technical Liaison Group works with standards bodies. Find more on ICANN at www.icann.org.
- **The Internet Society** (ISOC) is a nonprofit organization founded in 1992 to provide leadership in Internet standards, education, policy development, and advocacy. ISOC is the organizational home for the IETF. It is a global clearinghouse for Internet information and education; it coordinates related initiatives around the world; and it is dedicated to ensuring the open development, evolution and use of the Internet worldwide. Find more on ISOC at www.isoc.org.
- **Internet Governance Forum** (IGF) is a key outcome of the United Nations' World Summit on the Information Society (WSIS), held in 2003 and 2005. The IGF brings together governments, private sector, academia, and civil society in an informal, democratic and transparent structure. It has no oversight or decision-making functions. Rather, the objectives are to facilitate dialogue and find solutions to policy issues, to foster the sustainability and robustness of the Internet, and to facilitate development. The IGF started with a five- year mandate ending in September 2010. Find more on IGF at www.intgovforum.org/cms.

Other bodies that contribute to standards used in the Internet are the ITU, the Institute of Electrical and Electronics Engineers (IEEE), and the World Wide Web Consortium (W3C) for applications protocols.

This global governance framework reflects the decentralized, bottom-up, open nature of the Internet itself. While unwieldy in the view of many governments, like the Internet, *it works* and it enables continuous evolution. At its formation, ICANN was widely viewed as an experiment in governance of a global public resource. ICANN has had growing pains and there remain issues to be resolved, including the completion of its devolution from the U.S.

government. Still, CIRA believes that, on the whole, the global framework is a very successful governance model that we wish to see carried forward.

Canada has played an active role in the global framework. Many Canadians participate in the IETF, including Industry Canada officials. Canadians have been members of ICANN's Board of Directors, and Canadian companies and individuals participate regularly in the ICANN process. CIRA's President and CEO is the Vice-Chairperson of the Country Code Names Supporting Organization (ccNSO), with which CIRA is actively engaged. Industry Canada's current representative on ICANN's Governmental Advisory Committee (GAC) was recently appointed the Interim Chairperson, and a former Industry Canada representative was elected one of GAC's first two Vice-Chairpersons. Canadians have been on the Board of the Internet Society and are represented among its staff. The Government of Canada delegation to the WSIS was instrumental in devising the concept and mandate for the IGF and building support. Canadian government officials, businesses and non-governmental organizations have been ongoing and active IGF participants.

In short, CIRA believes that the current global framework for Internet governance works well and should be continued and strengthened. While some countries still push for an intergovernmental treaty organization, CIRA believes that this is unnecessary and likely to be detrimental. It is unnecessary because existing intergovernmental bodies with relevant expertise already participate in the current framework – notably the ITU, the Organization for Economic Cooperation and Development (OECD) and the World Intellectual Property Organization (WIPO). It would be detrimental for several reasons:

- The institutional burdens associated with intergovernmental bodies would increase costs, and slow down decision-making and the Internet's evolution.
- This approach would exclude or impair the open, transparent and equal participation of business, individuals and civil society, which has contributed greatly to understanding, capacity building and cooperation.
- Worse, it would replace bottom-up, expertise-driven coordination and management of critical technical resources with a top-down approach susceptible to political intervention, influence and trade-offs.
- It would undermine both the technical community and the continued rapid development and internationalization of the Internet.

Recommendation 5: The Government of Canada should continue to support the evolving, multi-stakeholder, de-centralised global Internet governance structure and oppose the transfer of these functions to an intergovernmental treaty organization whether existing or new.

Recommendation 6: The Government of Canada should exercise its influence within the UN to support continuation of the IGF for a further five-year mandate. Industry Canada should maintain or strengthen its participation in the organizations that make up this framework.

Domestic

It is not surprising to see significant Canadian participation in the global Internet governance framework. It is an approach that the Government of Canada has pursued since the early days of the Internet through initiatives including: the Information Highway Advisory Council (1994 to 1997); the Electronic Commerce Task Force (1999 to 2005); the Canadian Radio-television and Telecommunications Commission's (CRTC) New Media proceedings (1998/99 and 2007/08); the 2001 Cyberwise Strategy to Promote Safe, Wise and Responsible Internet Use; the Telecommunications Policy Review Panel (2005/06); and, the current Digital Economy consultations. Indeed,

Canada was an early adopter of, and has been a leader in, broad multi-stakeholder public forums for policy development related to the Internet.

Canada's open and consultative approach has enabled informed and ongoing updates to legislation, policies and programs and to cooperation in key areas. The government recognized early on that the Internet is not a "no-law land" and does not generally require specific legislation or regulation, but rather updating existing laws to ensure that they capture illegal online activity and provide for enforcement. An exception to this general rule is legislation to address spam and other on-line threats, but this too was developed through broad consultation. This light-handed approach is consistent with best-practices in countries where the Internet has flourished. It has also engendered partnerships to address Internet issues. CIRA itself came about through concerted action among Industry Canada, UBC and private sector Internet service providers (ISPs). The Cyberwise Strategy was another broad partnership. As well, two key contributors to Internet safety in Canada are non-governmental organizations jointly supported by the private sector and governments: *Media Awareness Network*, Canada's media and Web literacy authority and a recognized global expert www.media-awareness.ca; and Cybertip!ca, Canada's national tipline for reporting online sexual exploitation of children www.cybertip.ca.

A Canadian Internet Governance Forum: CIRA strongly supports the approach followed by the Government of Canada to date. We also believe that the success of the IGF model at the global level can be replicated in Canada to complement the government's approach and strengthen multi-stakeholder participation and cooperation. Domestic forums have been organized in a number of countries. Canada's active participation in the global IGF suggests that a Canadian IGF will attract wide interest. With this in mind, CIRA is organizing Canada's first domestic Internet Governance Forum, targeted for late 2010 to early 2011. It will include a series of focus groups to be held across Canada supported by an online discussion and followed by a national public discussion event, which will be webcast. Details will be announced soon on CIRA's website (www.cira.ca). The Government of Canada is, of course, a welcome participant.

> **Recommendation 7:** With respect to Internet governance in Canada, the Government of Canada should continue to pursue broad multi-stakeholder participation in the development of policy and legislation, a light-handed approach, and partnerships with the private sector and non-governmental organizations wherever appropriate.

> **Recommendation 8:** The Government of Canada should be an active participant in the forthcoming Canadian IGF.

Internet Regulation and Network Neutrality: CIRA supports the CRTC decisions to forbear from regulating ISPs under the *Telecommunications Act* and not to regulate the Internet under the *Broadcasting Act*. Canadians have benefited from these decisions through unfettered access to on-line services, contributing to economic development.

Complementary steps taken by the government and the CRTC to foster competition in wireline and wireless facilities have contributed to the rapid growth of Internet access, and stimulated deployment of broadband and other services. With respect to telecommunications and Internet policy reliance on market forces and fostering competition is central to the creativity/innovation value chain in Canada. However, CIRA suggests that from time to time there may be a role for governments to help foster or facilitate competition (such as the spectrum set aside).

CIRA believes that the CRTC was right to hold public hearings in response to Net Neutrality concerns.

Recommendation 9: With a view to safeguarding the Internet's openness, accessibility and capacity for dynamic, bottom up creativity and innovation, CIRA believes that the CRTC needs to be proactive and vigilant in ensuring openness, accessibility and fairness for both industry and consumers. The CRTC's principled and light-handed approach to regulation in its Net Neutrality decision is a first step in working to deter and, if required, remedy abuse.

Stability, Security and Resiliency

The Need for Action

Given the Internet's unprecedented rate of growth, it has proven to be remarkably robust, adaptable and resilient in responding to accelerating demands of e-mail, commercial transactions, social networking, voice and video services. Still, its underlying standards (protocols) were not designed to meet today's requirements.

The Internet's fundamental standards are the Internet Protocol Suite. These standards were developed with two primary goals in mind: first, to enable communication among widely distributed networks having different architectures by breaking up information into commonly recognized digital "packets"; and second, to ensure resiliency by allowing each packet to follow the most efficient path to its destination, routing around network bottlenecks or barriers. Since the intelligence to recombine packets into meaningful communications was located with end-users, the different underlying networks needed to provide only transmission. Security was not part of the design.

Similarly, the DNS was designed primarily to enable timely access to widely distributed information. In addition to mapping domain numbers to numerical IP addresses, the DNS supports other Internet directory-like functions to retrieve information for users. Multiple servers and local caches dynamically exchange and update data, providing redundancy, resiliency and robust service. Its original specifications did not include security largely because the DNS was designed to be a public database containing host names and IP addresses used to enable user access to information. So the concept of restricting access to information was purposely not part of the protocols.

The growth of e-commerce and increasingly sophisticated online applications created demand for more reliability, security, confidence, and real-time audio and video with no latency (jitter). In response, a plethora of innovative software solutions have been devised and deployed at various points in the network. Some mimic dedicated telecommunications channels to reduce latency in communications like voice; others compress large files like video to accelerate transmission; others manage traffic to accommodate many users and applications within finite bandwidth; still others, like firewalls and encryption, enable a surprisingly robust level of reliability and security and protect users and their equipment.

Nonetheless, there are limits even to the Internet's ability to accommodate exponential growth and adapt to more and more complex demands. The same openness that fosters innovation also enables criminal activity and destructive applications like viruses, spyware, malware, botnets and others that attack anything from e-mail to home computers to corporations and business transactions. As discussed in the following sections, efforts have been ongoing world-wide to update the Internet's underlying protocols to accommodate growth and address user needs. At the same time, governments have been updating laws and investigative techniques to combat online crime. *In the digital economy, stability, security and resiliency are critical to ensuring that the global, interconnected and interoperable Internet remains a dynamic driver of the creativity/innovation value chain.*

Recommendation 10: Governments in Canada and the private sector should develop strategies to deal with on-line threats and security issues and invest in technologies that safeguard on-line transactions.

Anti-SPAM legislation, copyright updates and others are important and timely as part of framework legislation to protect Canadians from illegal activity on-line just as they are protected from illegal activity off-line.

Recommendation 11: The Government of Canada should continue its efforts to update legislation with a view to building trust and confidence in the Internet, on-line transactions and the digital economy, while maintaining a light-handed approach to regulating the Internet.

Domain Name System Security Extensions (DNSSEC)

Given the functions that the DNS performs, the accuracy of information contained within the DNS is vital to many aspects of Internet communications and transactions. Yet its fundamental characteristics leave the DNS vulnerable to insertion of false information at various points. False information within the DNS can lead to unexpected and potentially harmful exposures. An attacker can inject bogus information into a DNS cache; establish a rogue server that redirects user queries to the wrong websites; or compromise an authoritative server. The result can be damaging information leakage, client flooding, denial of service, or redirection of users to sites that masquerade as a trusted entity and enable criminal activity.

In response to these threats, the IETF formed a working group in 1994 to add security "extensions" to the DNS protocol, commonly referred to as DNSSEC. These security enhancements are designed to be: interoperable throughout the DNS, backwards compatible, and able to co-exist with non-secure DNS implementations. The objectives of DNSSEC are to provide authentication and integrity to the DNS through the use of cryptographic signatures generated through public key technology.

DNSSEC allows an end-user to verify that the DNS information they have been presented with was published by the person who holds the private key for that domain, is authentic and has not been altered. Over 15 TLDs, including .GOV and .ORG and many country code top-level domains, are already using DNSSEC. CIRA began the process of implementing DNSSEC in early 2009. With trials in 2009 and implementation scheduled in 2011, users will have much greater assurance that .CA websites and email addresses are who they claim to be.

Recommendation 12: The Government of Canada should deploy DNSSEC to protect its online services to Canadians. In addition to being a model user, the government should promote the use of DNSSEC throughout the public and private sectors as part of a global, cooperative effort to build trust and confidence in the digital economy.

A Canadian DNS–Community Emergency Response Team (DNS-CERT)

Public Safety Canada is the federal government department responsible for national policy, response systems and standards for emergencies, including natural disasters, industrial accidents, terrorism, threats to Canada's electronic infrastructure from computer viruses and attack, and so on. To respond to these disasters, Public Safety works with partners and teams throughout Canada. The development of a broad-based emergency response team to ensure the safety and security of Canadian citizens and industry is key to ensuring the stability that underlies society.

The Internet's operation relies heavily on infrastructure such as the DNS. A widespread or persistent failure of infrastructure such as the DNS could render the Internet unusable by most individuals.

DNS failures are most often associated with malicious attacks. Some attacks have targeted specific corporations, websites or even top level domains. For example, in 2007, Estonia came under a huge Distributed Denial of Service (DDoS) attack. This attack, traced to Russia, involved one or more bot networks of tens of thousands enslaved computers. To stop the attack, many Estonian websites blocked international websites, resulting in significant impacts to Estonian business and society.

While a large number of existing organizations and activities currently support improving security awareness, response and resiliency across the DNS, no central Canadian authority exists to deal with Internet infrastructure security and coordinate action when needed. The creation of a Canadian Domain Name System–Community Emergency Response Team (DNS-CERT) devoted to both proactive and reactive measures related to DNS security, stability and resiliency would lessen the impact of future attacks against or failures of the system and be a first step to a potentially larger CERT.

As manager of the .CA ccTLD, CIRA is in a position to identify rapidly the source of an attack that originates from within the .CA domain. For this reason, CIRA is well equipped to assist with the establishment of a DNS-CERT, including providing expert advice on its set up. Such a CERT would require cross-industry consultation and input from relevant stakeholders, enforcement authority, adequate information sharing, and strategic direction to provide a strong cybersecurity program.

> **Recommendation 13:** A DNS-Community Emergency Response Team (DNS-CERT) should form part of the Government of Canada's emergency response strategy. CIRA is ready to assist the government, law enforcement authorities and the private sector in the development of a Canadian DNS-CERT.

Internet Protocol Version 6 (IPv6)

The version of the Internet Protocol currently in use, IP version 4 (IPv4) can accommodate about four billion addresses. This was thought to be sufficient before the explosive growth of the World Wide Web. However, by the late 1980s, methods were already being developed to conserve address space and in the 1990s work began on a new version of the IP. Although various techniques and sharing of IP addresses have significantly extended the capacity of IPv4 to accommodate the growth in Internet users, the central Internet Assigned Numbers Authority (IANA) registry and its affiliated regional registries worldwide now are forecasting IP address exhaustion sometime in 2011. Moreover, IPv4 was not designed to accommodate security features within its basic design components.

The replacement for IPv4 is IPv6 (v5 was leapfrogged), which has a vastly larger address space. This results from the use of a 128-bit address, compared to 32 bits in IPv4. The new address space thus supports 2^{128} (about 3.4×10^{38}) addresses. This expansion provides tremendous flexibility in allocating addresses and routing traffic, a necessity as more appliances and devices are connected to the Internet. Equally important, the new protocol is designed to accommodate network security and reliability features not provided for in IPv4. It will also accommodate functionalities not currently available in IPv4, including network intelligence and quality of service features important for low-latency applications like voice and video. As well, it enables improved mobile services, perhaps the fastest growing Internet applications. IPv6 is already being deployed in a range of Internet applications.

One might think that such a vastly improved protocol would be widely and quickly adopted, but this has not been the case for several reasons. As noted earlier, methods were introduced to conserve address space; as well, many IP addresses are actually reused and recycled daily (each time someone logs on and off, their ISP issues and then takes back an IP address, allowing addresses to be shared many times in a day). So the pressure building on address space is not readily apparent. Cost is another factor, since deployment of IPv6 requires modifications to software and

equipment throughout the Internet access chain. As well, given the many ongoing users and uses of IPv4 addresses, both versions will need to be operational for an extended transition period. So, companies ranging from small ISPs to major carriers, users and even governments have not had a compelling incentive to deploy IPv6. Faced with address space exhaustion within a year, this complacency cannot be sustained.

CIRA has already begun implementing IPv6 and currently has the capability to resolve IPv6 applications. Full deployment is expected to be completed within 12 to 18 months. However, within both the private and public sectors in Canada, investment in and deployment of IPv6 equipment has been slow. CIRA was therefore pleased to see in the Digital Economy Consultation Paper that the Government of Canada is working with major stakeholders to plan its own adoption of IPv6 solutions.

> **Recommendation 14:** Governments should take a leadership role by deploying IPv6, promoting awareness, leveraging their purchasing power to stimulate IPv6 adoption, and using tax policy to encourage the transition from IPv4 to IPv6. Government use will stimulate demand among its private sector suppliers and users of government services. CIRA looks forward to participating in the Government of Canada's discussions with stakeholders on its plan for IPv6 adoption.

DNS Redirection

When an Internet user types a domain name into a Web browser and clicks the search button, most of the time the user arrives at the expected website. But if the user makes an error typing in the address, or the address is non-existent, he or she should get a "Page not found" notice, also known as "NXDomain". This is the manner in which the Internet Protocol was designed, and intended outcome of the relevant Request for Comments (RFCs). However, over time many organisations, including commercial ISPs began "redirecting" such non-existent queries to a page that they control which often contains links to other related sites with which the ISP has a commercial relationship.

Sometimes the ISP is transparent about its use of DNS redirection, attempting to brand it as a helpful service. However, the result is harmful and users are usually unaware of this behaviour. Some of the harmful outcomes of this practice include the following:

- Users not receiving notification of bounced e-mails or transactions.
- Spam and anti-virus filters either not working properly or not at all.
- Difficulties with troubleshooting: very long delays, perhaps days or weeks, before even trivial errors are brought to the user's attention.
- Additional charges: where Internet access fees are volume-based (most wireless data services), users may be billed for bandwidth to access both the site they wanted to see and the site to which the ISP redirected them.

There are many architectural assumptions around the DNS that are not specified in standards, but that are deeply embedded in the way Internet protocols and applications work. As a proponent of DNS stability, security and resiliency, and of protecting user trust and confidence in the Internet, CIRA strongly disagrees in principle with interfering with the norms upon which the Internet was built. The overall consensus from the international Internet community is that DNS redirection should prohibited, with the exception of rare instances for purposes of law enforcement.

Further, such interference may put at risk the security and stability of the network by preventing wide spread deployment of protocols such as DNSSEC that rely on DNS data not being modified while in transit.

Recommendation 15: The Government of Canada should encourage Canadian ISPs to cease the practice of DNS redirection. In CIRA's view, voluntary action would be preferable to regulatory intervention or an eventual legal liability, but the practices must be discontinued, except in rare cases involving law enforcement.

Infrastructure, Metrics, Digital Media and Skills for Tomorrow

Infrastructure and Metrics

- Industry Canada question: *What speeds and other service characteristics are needed by users (e.g., consumers, businesses, public sector bodies and communities) and how should Canada set goals for next generation networks?*
- Industry Canada question: *What steps must be taken to meet these goals? Are the current regulatory and legislative frameworks conducive to incenting investment and competition? What are the appropriate roles of stakeholders in the public and private sectors?*

Infrastructure: CIRA is concerned that, despite the relatively widespread availability of broadband access networks in Canada, the cost per megabyte, and service gaps in rural and remote areas, are barriers to the digital economy value chain. The government has taken and is taking steps to help deploy infrastructure to under-served areas. However, even in urban areas, bandwidth costs per megabyte, particularly for business users, are too high compared to other countries.

OECD data suggest that Canada's average monthly price for one megabyte per second (mbps) service is $6.50 U.S. This is almost twice the rate in the U.S. and higher than in most major European countries. As for average speed, available data from the same source show Canada at 7.6 mbps, which is better than U.S. (4.8) and comparable to most European countries, but still significantly behind Japan, Korea, Sweden, Finland, and France.

CIRA's own experience in acquiring network and server capacity demonstrates this concern. For example, CIRA's experience has shown that transit prices are typically 2.5 to five times higher in Canada than in the U.S. Moreover, with respect to co-location services in Ottawa, CIRA was unable to obtain the capacity that it needed. For this reason, it was more economical for CIRA to build its own server room. In U.S. cities of comparable in size to Ottawa, competitive options are available. CIRA is concerned that in Canada, the high cost of bandwidth makes it uneconomic for competitive data centres to establish here.

As noted in the section on regulation, CIRA believes that Canada has benefited from its policy to rely on market forces and promote competition in telecom networks and services. There is no question that competition between the telephone and cable-TV companies made Canada an early leader in the deployment of first generation broadband networks. CIRA does not advocate a return to regulation to address concerns about deployment of next generation networks and costs per megabyte.

In its policy framework for the 2008 auction of radio frequency spectrum, Industry Canada set aside spectrum for new entrants and adopted other measures to foster new market entry. At that time, Industry Canada stated, "The department must consider whether the market, and in particular consumers, could benefit from further competition which would strengthen Canada's ability to rely on market forces to the maximum extent feasible," and that " . . . ensuring opportunities for new facilities-based entrants into telecommunications markets is therefore an important policy issue." Stated differently, a policy to rely on market forces benefits consumers most when markets are as competitive as they can be. CIRA concurs.

Recommendation 16: In developing its policies related to telecommunications and the Internet, the Government of Canada should always consider whether the market, and in particular consumers, could benefit from further competition which would strengthen Canada's ability to rely on market forces to achieve continued innovation In keeping with its Policy Direction to the CRTC, the government should carefully consider whether policies that impede new entry into telecommunications markets, such as investment restrictions, are efficient and proportionate to their purpose and whether the objectives underlying such policies can be achieved by other measures that interfere with the operation of competitive market forces to the minimum extent necessary. The government should bear in mind that Canadians benefit most from reliance on market forces when markets are fully and dynamically competitive.

Metrics: As a general rule, what gets measured gets managed. Benchmarking Canada's performance in the digital economy against other countries, and in particular against major trading partners, is essential to assessing competitiveness. As a relatively small economy heavily dependent on trade to support its economic growth, it is very important for Canada to at least keep up. Showing leadership would be even better. The pace of change in the digital economy and the digital value chain is so fast that falling behind can quickly undermine performance and catching up with a speeding train is hard.

In saying this, CIRA fully acknowledges that international comparisons are fraught with difficulty and that often different methods and studies come up with differing results. Nonetheless, the objective is not to criticize the messenger, but rather, to identify trends that may be of concern. When a number of leading indicators all show weakness in a given area, that should be a signal for action by government, the private sector or both. Government can play a role by undertaking research and analysis to identify the source of the problem and determine what government measures may be appropriate. Businesses can use the benchmarking to improve productivity and competitiveness – both their own and that of their suppliers.

Recommendation 17: CIRA believes that it is useful for the Government of Canada to benchmark Canada's performance in the digital economy against other countries and in particular against major trading partners. With this in mind, it might be useful to create an ongoing compendium of publicly available data with an annual assessment of where Canada stands, available on-line.

Digital Media

- Industry Canada question: *What does creating Canada's digital content advantage mean to you?*
- Industry Canada question: *What are the core elements in Canada's marketplace framework for digital media and content? What elements do you believe are necessary to encourage the creation of digital media and content in both official languages and to reflect our Aboriginal and ethnocultural communities?*
- Industry Canada question: *How do you see digital content contributing to Canada's prosperity in the digital economy?*

As the CRTC's two new media proceedings (1998/99 and 2007/08) demonstrated (both in submissions received and in the final reports) digital content and media are fields where Canada has significant competitive advantage. The record of the second proceeding reveals how rapidly digital content and media expanded in the intervening years under the CRTC's enlightened initial decision not to regulate. CIRA is of the view that this was both the correct and only practical decision given the nature of the Internet. Two studies done for Industry Canada over the same period concluded that content regulation on the Internet would be hugely expensive, easily bypassed, and would impose significant costs across the entire economy. See: Regulating the Internet – A Technological Perspective, 1999

(http://www.ic.gc.ca/eic/site/smt-gst.nsf/vwapj/05082-eng.pdf/$FILE/05082-eng.pdf) and Regulating the Internet - A New Technological Perspective 2008 (http://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf09030.html).

Despite maintaining its decision not to regulate Internet content in 2008, the CRTC has initiated proceedings in the Federal Court to obtain clarity as to whether or not it can regulate ISPs under the *Broadcasting Act*. This arises from the view expressed by some in the CRTC proceeding that, with video content increasing on the Internet, ISPs are analogous to broadcasting distributors like cable-TV and satellite services and that they should pay the same levy (generally five per cent of broadcasting revenues) to support Canadian content. CIRA is not a participant in this court case, which is beyond our expertise. *However, we continue to be of the view that the CRTC got it right the first time and that the Internet is no place for broadcasting regulation*.

CIRA is fully supportive of policy objectives to support and promote Canadian content. However, current broadcasting law, policy and regulation stem from the 1986 Report of the Caplan-Sauvageau Task Force – more than a generation ago in years and considerably more in the evolution of communications technologies. As several CRTC reports and other studies have shown, the Internet has changed the fundamental technological premises upon which the 1991 *Broadcasting Act* is based. The policy objectives spelled out in the Act reflect concerns arising from a market and technologies characteristic of a vastly different era when audio and video content were accessible only from local over-the-air TV and radio, cable-TV and big satellite dishes.

> **Recommendation 18:** The Government of Canada should undertake a comprehensive review of broadcasting law, policy and regulation in the context of the interactive, digital, global Internet. The review should consider whether existing measures are still useful and effective in pursuing policy objectives for Canadian content in the current environment and, if not, what other measures would be more effective while interfering minimally with the Internet and the digital economy. The CRTC should maintain its exemption for the Internet and new media, taking into account the potential negative impact of applying measures conceived in and for another era.

Skills for Tomorrow

- Industry Canada question: *What do you see as the most critical challenges in skills development for a digital economy?*
- Industry Canada question: *What is the best way to address these challenges?*

The consultation document notes that Canada has fallen behind a number of other countries in the development of the digital economy. As well, in several places, the government's consultation paper acknowledges the need for digital skills development. For example, at page 13:

> "…There is also evidence that smaller firms are adopting less rapidly than larger ones when it comes to more advanced ICT applications… It is not clear whether some SMEs do not adopt more complex applications because they do not see value in adopting them, or rather, whether it is because the ICT solutions already in the marketplace do not serve SME needs. "

And again at page 27:

> "…With a near-constant evolution of technologies, and an emerging industry comprised often of small and medium-sized companies, the Government of Canada recognizes that there is a need to develop skills, and share expertise and best practices."

In context, the second reference is about the cultural/new media sector, but CIRA believes that it applies to many emerging sectors in the digital the economy. The pace of change in digital technologies is so rapid that staying at the

cutting edge of digital literacy – where innovation takes place – requires ongoing and continuous training and skills updating. Digital literacy therefore needs to be understood as a lifelong pursuit that is essential for success, productivity and competitiveness.

CIRA believes that there is a link between Canada falling behind and digital literacy. While this is not an area of expertise for CIRA, as a supporter of the Media Awareness Network (MNet), we are aware that this link is explored in considerable depth in MNet's submission to Industry Canada. CIRA supports MNet's conclusion that there is a connection between Canada's declining performance in the digital economy and our failure to develop a national digital literacy strategy.

> **Recommendation 19:** The Government of Canada, in partnership with provincial governments, the private sector and others with relevant expertise, should develop a digital literacy strategy for Canada as part of its overall strategy for the digital economy. With this in mind, CIRA commends the submission of the Media Awareness Network for careful consideration.

List of Recommendations

Recommendation 1: The .CA domain name extension is a visible marker of online security, and the Canadian government should champion use of it by:

- Requiring all websites developed by or contracted by the government use the .CA domain name extension.
- Encouraging partner and arms length organization use the .CA domain name extension.
- Encouraging use of the .CA domain name extension by Canadians through its related communications materials.

Recommendation 2: The Government of Canada's digital economy strategy should focus on providing a foundation that enables innovation across the whole economy, by updating laws and regulations to ensure confidence and trust in on-line transactions, by removing barriers to the digital economy value chain wherever it can, and where demonstrably required, by providing targeted incentives that foster creativity and innovation, in particular for research and development.

Recommendation 3: The Government of Canada undertake research to assess whether specific market conditions in Canada impede adoption and/or whether aspects of Canada's fiscal and tax framework can be modified to spur adoption of ICT by Canadian businesses and public sectors.

Recommendation 4: Governments in Canada should develop strategies to become more informed and demanding users of ICTs and the Internet.

Recommendation 5: The Government of Canada should continue to support the evolving, multi-stakeholder, de-centralised global Internet governance structure and oppose the transfer of these functions to an intergovernmental treaty organization whether existing or new.

Recommendation 6: The Government of Canada should exercise its influence within the UN to support continuation of the IGF for a further five-year mandate. Industry Canada should maintain or strengthen its participation in the organizations that make up this framework.

Recommendation 7: With respect to Internet governance in Canada, the Government of Canada should continue to pursue broad multi-stakeholder participation in the development of policy and legislation, a light-handed approach, and partnerships with the private sector and non-governmental organizations wherever appropriate.

Recommendation 8: The Government of Canada should be an active participant in the forthcoming Canadian IGF.

Recommendation 9: With a view to safeguarding the Internet's openness, accessibility and capacity for dynamic, bottom up creativity and innovation, CIRA believes that the CRTC needs to be proactive and vigilant in ensuring openness, accessibility and fairness for both industry and consumers. The CRTC's principled and light-handed approach to regulation in its Net Neutrality decision is a first step in working to deter and, if required, remedy abuse.

Recommendation 10: Governments in Canada and the private sector should develop strategies to deal with on-line threats and security issues and invest in technologies that safeguard on-line transactions.

Recommendation 11: The Government of Canada should continue its efforts to update legislation with a view to building trust and confidence in the Internet, on-line transactions and the digital economy, while maintaining a light-handed approach to regulating the Internet.

Recommendation 12: The Government of Canada should deploy DNSSEC to protect its online services to Canadians. In addition to being a model user, the government should promote the use of DNSSEC throughout the public and private sectors as part of a global, cooperative effort to build trust and confidence in the digital economy.

Recommendation 13: A DNS-Community Emergency Response Team (DNS-CERT) should form part of the Government of Canada's emergency response strategy. CIRA is ready to work with government, law enforcement authorities and the private sector to develop a Canadian DNS-CERT.

Recommendation 14: Governments should take a leadership role by deploying IPv6, promoting awareness, leveraging their purchasing power to stimulate IPv6 adoption, and using tax policy to encourage the transition from IPv4 to IPv6. Government use will stimulate demand among its private sector suppliers and users of government services. CIRA looks forward to participating in the Government of Canada's discussions with stakeholders on its plan for IPv6 adoption.

Recommendation 15: Industry Canada should encourage Canadian ISPs, either individually or as a group, cease the practice of DNS redirection. In CIRA's view, voluntary action would be preferable to regulatory intervention or an eventual legal liability, but the practices must be discontinued, except in rare cases involving law enforcement.

Recommendation 16: In developing its policies related to telecommunications and the Internet, the Government of Canada should always consider whether the market, and in particular consumers, could benefit from further competition which would strengthen Canada's ability to rely on market forces to the maximum extent feasible. In keeping with its Policy Direction to the CRTC, the government should carefully consider whether policies that impede new entry into telecommunications markets, such as investment restrictions, are efficient and proportionate to their purpose and whether the objectives underlying such policies can be achieved by other measures that interfere with the operation of competitive market forces to the minimum extent necessary. The government should bear in mind that Canadians benefit most from reliance on market forces when markets are fully and dynamically competitive.

Recommendation 17: CIRA believes that it is useful for the Government of Canada to benchmark Canada's performance in the digital economy against other countries and in particular against major trading partners. With this in mind, it might be useful to create an ongoing compendium of publicly available data with an annual assessment of where Canada stands, available on-line.

Recommendation 18: The Government of Canada should undertake a comprehensive review of broadcasting law, policy and regulation in the context of the interactive, digital, global Internet. The review should consider whether existing measures are still useful and effective in pursuing policy objectives for Canadian content in the current environment and, if not, what other measures would be more effective while interfering minimally with the Internet and the digital economy. The CRTC should maintain its exemption for the Internet and new media, taking into account the potential negative impact of applying measures conceived in and for another era.

Recommendation 19: The Government of Canada, in partnership with provincial governments, the private sector and others with relevant expertise, should develop a digital literacy strategy for Canada as part of its overall strategy for the digital economy. With this in mind, CIRA commends the submission of the Media Awareness Network for careful consideration.