Information Technology Industry Council

August 24, 2012

Josée St-Onge
Public Works and Government Services Canada
Network and Satellite Services Division
11 Laurier St.
Place du Portage, Phase III
Tower C – Office 12CI – 102- 62
Gatineau, Quebec, K1A 0S5 CANADA

Via fax and e-mail to: 819-997-9776 and josee.st-Onge@tpsgc-pwgsc.gc.ca

RE: Concerns Regarding Shared Services Canada's *Integrated Communications and Support Services (ICCS), Solicitation # 2B0KB-130262/A*

Dear Ms. St-Onge:

The Information Technology Industry Council (ITI) is writing to express concerns with Shared Services Canada's bid solicitation referenced above. Note this is not a bid on the solicitation itself.

ITI is the premier voice, advocate, and thought leader in the United States for the information and communications technology (ICT) industry. ITI's members[1] comprise the world's leading technology companies and collectively provide the full range of voice over Internet protocol (VOIP) products, accessories, and parts and related support services referenced in this bid solicitation. Further, our members are global companies located in various countries. Most service the global market and have extensive global supply chains in which products are developed, made, and assembled in multiple countries across the world. As a result, we have an acute understanding of the impact of international policies on security innovation and of the need for all governments' policies to be globally consistent. In addition, as both producers and consumers of ICT products and services, our members have extensive experience working with governments around the world on the critical issues of cybersecurity policy and government procurement. Our industry shares the goal with governments of improving cybersecurity and therefore our interests are fundamentally aligned. In fact, for over a decade, ICT companies have provided leadership, subject matter experts, technical and monetary resources, and innovation to work with governments to better manage and mitigate cybersecurity risk.

We are writing to express concern with Canada's general invocation of a National Security Exception in its trade agreements, and how that exception applies to this particular project, notably the requirement that bidders only supply hardware and software designed, assembled, and integrated in a finite list of approved countries. In short, we think that basing a security determination on country of origin does not truly equate with security, and has important negative implications on both security and trade. We strongly encourage Canada to use objective criteria in its procurements to determine if a product is appropriate for a particular use. In fact, this RFP includes a number of security and privacy requirements for the network

[1] See attached list of ITI member companies.

products and support services outlined in the statement of work, and Canada should consider those requirements sufficient for this project.

National Security Exception: General Concerns[2]

SSC states that the bid solicitation "is subject to National Security Exception and is, therefore, excluded from all of the obligations of the trade agreements." According to SSC's May 25, 2012, memo, *Notification to Suppliers: National Security Exception for E-Mail, Network, and Data Centre Systems, Infrastructure and Services*, "Public Works and Government Services Canada, at the request of Shared Services Canada (SSC), has invoked the National Security Exception under Canada's domestic and international trade agreements in connection with procurements for SSC related to e-mail, network/telecommunications and data centre systems, infrastructure and services. This is part of a Government of Canada strategy to create a secure, centralized communications infrastructure."

We are extremely concerned about Canada's invocation of the National Security Exception to avoid its international trade obligations related to procurements. While we support Canada's desire to seek a secure government communications infrastructure, we fear that by invoking the National Security Exception Canada will embolden other countries—such as India, Brazil, and China-- to assert such exceptions to their own trade obligations. This could have a significant negative impact on global ICT vendors, including those based in Canada and the United States, that rely heavily on sales in those large and growing markets to maintain domestic jobs. Although countries such as India, Brazil, and China are not signatories to the World Trade Organization (WTO)'s Government Procurement Agreement, they have made WTO commitments to treat foreign and domestic products the same when sold in the their commercial markets. Unfortunately, those countries have begun to take actions that would shut foreign ICT companies out of their markets in order to build up domestic ICT champions, often relying explicitly or implicitly on national security as the rationale for their regulatory initiatives. For example, in February 2012 India's Department of Information Technology released a Preferential Market Access (PMA) notification, mandating preferences for domestically manufactured electronic goods for the purpose of government procurement as well as for products that have undefined "security implications." China has issued a rash of information-security-related national standards and policies related to ICT security that discriminate against foreign technologies, citing national security concerns.

In short, if these countries emulate Canada, it could contribute to a "race to the bottom" whereby country after country invokes a similar rationale to justify excluding foreign companies or technologies from their markets, which would significantly disrupt global trade. In fact, we understand Canada's actions to invoke its National Security Exception has been reported in the Chinese press and also has come to the attention of the Indian Government.

[2] ITI voiced these same concerns with the NSE in our July 23, 2012 response to SSC's *Email Transformation Initiative: Request for Information*, which also was issued under the umbrella of the May 2012 NSE memo.

National Security Exception: Specific Concerns Related to this Project

In this particular bid solicitation, Canada's National Security Exception is being used to justify restricting prospective providers to those that can attest that the "design, assembly and integration of sub-assemblies of hardware and licensed software composing the information systems proposed" in their bids occur in a finite list of countries. We understand that SSC revised the bid solicitation in July by expanding the number of qualified countries from 3 to 29, [3] and modifying the production and manufacturing functions that could occur, after questions or complaints from industry. The addition of approved countries and amendment of activities does not, however, mitigate our concerns.

First, the restrictions in this bid proposal on hardware and software country of origin, like SSC's National Security Exception generally, send a very troubling message to Canada's trading partners that such an approach is acceptable or is thought to improve security. Per the *Global Information and Communications Technology (ICT) Industry Statement: Recommended Government Approaches to Cybersecurity, June 2012*,[4] governments should allow for procurement of technologies regardless of the country of origin or the nationality of the technology vendor because product security is a function of how a product is made, used, and maintained, rather than by whom or where it is made. In fact, the RFP contains 209 security and privacy requirements[5] in Appendix B (Annexes, pp. 84-110), and a number of security certification and accreditation requirements in Appendix C (Annexes, pp. 111-112). From a security perspective, SSC should judge bids on the basis of whether they meet these requirements, not on country of origin. It is imperative that Canada set an example for others around the world on how address legitimate cyber security concerns without disrupting innovation, competition, and global trade flows.

Second, application of the National Security Exception in this situation is overbroad. If the network products and support services in question were processing information only at an extremely sensitive level (e.g. they were supporting secure communications), a national security designation and potential exception could be justified. However, the bid solicitation applies to systems that may process much broader categories of less sensitive information. Per item 7.5 (f) (a), General Security Measures Surrounding Transmission of Sensitive Data (p. 23):

> *The Network Products and support services provided under the Contract will be used for the transmission of Government of Canada* ***data of various kinds, and may include*** *secure communications (at various security classification levels), privileged communications (such as Cabinet confidences and solicitor-client communications), and otherwise sensitive communications (including transmissions containing personal information of Canadians*

[3] Albania, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Lithuania, Luxembourg, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Turkey, United Kingdom, United States, and Mexico.

[4] *Global Information and Communications Technology (ICT) Industry Statement: Recommended Government Approaches to Cybersecurity, June 2012*. Issued by the Information Technology Industry Council (ITI), DIGITALEUROPE, and the Japan Electronics and Information Technology Industries Association (JEITA). See http://www.itic.org/dotAsset/51ad6069-9f1b-4505-b2ff-b03140484586.pdf.

[5] For example, item # 157, identifier SA-13, requires Common Criteria EAL+1 validation for IP-enabled network products. The CC is the global standard for product assurance.

and proprietary or confidential information of third parties, such as suppliers)" (emphasis added).

Asserting a national security exception should be reserved for very narrow and clearly justifiable cases, not applied generally to projects where great portions of that project have no palpable national security interest. The global ICT industry's statement on government approaches to cybersecurity referenced above recommends that governments "Limit any prescriptive requirements to areas of the economy that are highly sensitive, such as government intelligence and military networks . . . Government procurement requirements for such systems should not extend to other government networks, government-licensed networks or to privately run infrastructure or commercial companies."

Third, the approach Canada is taking ironically could lead to decreased security of the Canadian Government's information systems. Invoking a blanket National Security Exception and country of origin restrictions will restrict the government's list of qualified suppliers and technologies. In addition, if too many onerous conditions are placed on government bidding, companies able to provide qualified products and services may decide that it is not worth the trouble. Consequently, Canada may not have access to the widest range of leading-edge security technologies available. Similarly, given that the requirements are more applicable to GOTS products, the end result is higher costs, limited interoperability, less innovation, and fewer ICT suppliers available to the Canadian Government.

Finally, the limitation that the "design, assembly and integration of sub-assemblies of hardware and licensed software" come from specific countries is incompatible with the way modern ICT companies operate. The ICT sector has spent years creating complex and efficient hardware and software product development, manufacturing, and assembly supply chains that span the globe (including many countries that are not on the list) that respond dynamically to a variety of user needs and conditions. Further, some products include open source software that is wide open for global input, with no practical way to determine "nationality." It is unrealistic to expect ICT companies to create or maintain supply chains that only allow for sub-assemblies and products from a list of approved countries. This requirement is even more unworkable given the RFP's contradictory requirement that, per Section 5.3 (p. 17), the bidder must certify that its system is "Off-the-Shelf" in that it is commercially available. The creation or maintenance of supply chains that only source from a finite list of countries would require companies to expend extraordinarily large resource commitments and customizations that are much more suitable for custom-designed government-off-the-shelf (GOTS) products, not commercial-off-the-shelf (COTS) products.

Conclusion

ITI companies are committed to working with our government partners to improve cybersecurity. We welcome the opportunity to talk with SSC and other Canadian Government entities about global approaches to secure government information systems that are based on best practices as opposed to regulations that hinder market competition. Please consider ITI and its member companies a resource for the Canadian Government on cybersecurity issues moving forward. Do not hesitate to contact me at any time with any questions at dkriz@itic.org or +1-202-626-5731.

Sincerely,

Danielle Kriz
Director, Global Cybersecurity Policy

CC: Foreign Affairs and International Trade Canada (DFAIT)

Information Technology Industry Council

2012 Member Companies

accenture
High performance. Delivered.
Adobe
Agilent Technologies
Alcatel·Lucent
ALTERA
AMD
Aol.
Apple Inc.
APPLIED MATERIALS
Autodesk
BROADCOM.
Canon
ca technologies
cisco
Cognizant
CORNING
DELL
ebay
EMC²
ERICSSON
FUJITSU
Google
hp
IBM
intel
intuit
Kodak
lenovo
LEXMARK
Micron
Microsoft
monster.com
MOTOROLA
NCR
NOKIA
ORACLE
Panasonic
ideas for life
QUALCOMM
RICOH
RIM
SAP
Schneider Electric
SONY
Symantec
SYNOPSYS
TERADATA
Raising Intelligence
Texas Instruments
VERISIGN
vmware

Information Technology Industry Council
1101 K St, NW Suite 610, Washington, D.C. 20005
T +1 (202) 737-8888, wwww.itic.org

Innovation. Insight. Influence.