Information Technology Industry Council

July 23, 2012

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

Via e-mail to: jason.knowles@pwgsc-tpsgc.gc.ca

RE: Response to Shared Services Canada's *Email Transformation Initiative: Request for Information, Solicitation # 2B0KB-123327/B*

Dear Mr. Knowles:

The Information Technology Industry Council (ITI) appreciates the opportunity to respond to Shared Services Canada's (SSC) Request for Information (RFI) pertaining to the Email Transformation Initiative.

ITI is the premier voice, advocate, and thought leader in the United States for the information and communications technology (ICT) industry. ITI's members comprise the world's leading technology companies, many of which provide products and services that comprise e-mail solutions, including IT systems, communications networks, servers, and server and client applications. Further, our members are global companies. Most derive a substantial portion of their revenues from foreign markets and have extensive global supply chains. As a result, we have an acute understanding of the impact of international policies on cybersecurity innovation and of the need for all governments' policies to be consistent with international norms. Further, 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. The interests of industry and governments in improving cybersecurity are fundamentally aligned.

We understand that SSC and Public Works and Government Services Canada seek feedback from industry on four main topics related to the RFI. We are most concerned with, and will comment on, the more general National Security Exception. We also provide responses to portions of sections (i) and (ii).

National Security Exception

SSC states that "The procurement related to this initiative is subject to National Security Exception and is, therefore, excluded from all of the obligations of the trade agreements." This Exception was described in more detail in a May 25, 2012 memo from SSC, *Notification to Suppliers: National Security Exception for E-Mail, Network, and Data Centre Systems, Infrastructure and Services.* The memo states:

> *This notification is being published in order to inform suppliers that 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 with regard to its international trade obligations. In invoking such exceptions, Canada asserts its rights to, among other things, pre-select suppliers. 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, and others-- to begin to be more aggressive in asserting such exceptions to their WTO obligations. This could have a significant negative impact on global ICT vendors, including those based in Canada and the United States, that rely on sales in those large and growing markets. 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 related to fairly treating foreign companies that wish to participate in their commercial markets. Unfortunately, they have begun to take actions that would shut foreign ICT companies out of their markets, often using national security as rationale, which skirts very closely to taking similar trade obligation exceptions. 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." Brazil recently included local manufacturing and locally developed technology requirements into its specifications for companies to bid on fourth generation (4G) telecommunications spectrum. 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 a "race to the bottom" whereby country after country invokes similar rationale to justify shutting foreign companies or technologies out of their markets, which would 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 come to the attention of the Indian Government.

The application of the National Security Exception to this particular RFI is notably troublesome due to the RFI's broad scope. If the e-mail system in question were processing e-mails only at an extremely sensitive level (e.g. Secret), a national security designation and potential exception could be understood. However, the ETI's e-mail system is meant to process a much broader and less sensitive set of e-mails. Per the RFI's section 6.1.2, the scope includes "Secret system (which includes Classified information up to Secret and/or Protected information up to Protected C), and/or a Protected system, up to and including Protected B." On July 16, SSC issued Amendment #7 (PW-$TSS-002-24571) in response to a question regarding how these classifications map to those in the United States. SSC responded: "There is no formally accepted GC standard mapping Canadian classification to US classification. Based on [Communications Security Establishment Canada] CSEC's policies and experience exchanging information with the US and the knowledge of their handling requirements, this mapping should be used in the context of the ETI project:

Canadian Marking	**Equivalent US Marking**
Unclassified	Unclassified
Protected A	Unclassified//FOUO (For Official Use Only)
Protected B	Confidential
Protected C	Secret

Confidential	Confidential
Secret	Secret
Top Secret	Top Secret"

We question whether e-mails considered unclassified rise to the level of national security. While it certainly is important that all government e-mails be appropriately secured, the level of security required should be commensurate with the risks involved. 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. Per the *Global Information and Communications Technology (ICT) Industry Statement: Recommended Government Approaches to Cybersecurity, June 2012*, we recommend that governments "Limit any prescriptive requirements to areas of the economy that are highly sensitive, such as government intelligence and military networks. Many governments may justifiably have very stringent requirements for security technologies sold into 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.[1]

In addition to the aforementioned concerns, it is important to note that the approach Canada is taking could also lead to decreased security of the Canadian Government's information systems—the opposite of what Canada intends. Invoking a blanket National Security Exception, which then is used to justify various constraints on bidders, will likely restrict the suppliers or technologies from which the government may procure. This in turn means that Canada may not have access to the widest range of leading-edge security technologies available. It is imperative that governments such as Canada set an example for others around the world as to the importance of allowing global competition in their markets.[2]

Our companies are committed to working with our government partners to improve cybersecurity. We would welcome the opportunity to talk with SSC and other Canadian government entities about global approaches to security of government information systems that are based on best practices as opposed to regulations that hinder market competition.

---

[1] *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

[2] Although outside the scope of this ETI RFI, we also would like to state our concerns with the use of this National Security Exception for other projects. SSC's RFP for "Integrated Communications and Support Services (ICSS) – for IP Telephony Equipment and Service," requires that bidders certify that the design, assembly, and integration of sub-assemblies of hardware and licensed software composing the information system proposed in its bids occur withn one or more" of a list of 29 countries (although the components of the information system can be manufactured outside of this list). The security of technology and services is not dependent on by whom, or where, the products or services are made. Rather, security is a function of how products or services are produced, procured, and maintained.

(i): The Ability to meet the anticipated mandatory requirements provided in Part III of the RFI

13: SECURITY REQUIREMENTS

13.4 Canadian Citizenship for Support Personnel

All engineering and technical support personnel must be Canadian citizens.

We respectfully disagree that Canadian citizenship should be required for all engineering and technical support personnel. First, the security of technology and services is not dependent on by whom, or where, the products or services are made. Rather, security is a function of how products or services are produced, procured, and maintained. Restricting the pool of engineering and technical support talent to Canadian citizens could mean that the bid winner (and all of its subcontractors) will have only a limited pool of talent from which to choose. While we have no doubt Canada has a large number of talented engineers, it is very possible that skill sets needed for certain tasks could reside in companies' non-Canadian citizen workforces.

Second, given the complexity of ICT product development and global supply chains it is highly unlikely that companies could document the nationality of every single person involved in a technology's design and development. This is particularly true for software, where different components of the product may be actively developed in different locations. Further, some products include open source software that is wide open for global input, with no practical way to determine "nationality."

Finally, as with our comments above on Canada's very broad application of national security exception to this e-mail project, a broad mandate regarding all personnel is equally troubling. It is imperative to be judicious regarding which positions related to this project genuinely need parameters around them, including citizenship. Echoing our comments made earlier, while we support Canada's desire to seek a secure government communications infrastructure, we fear that Canada issuing a blanket requirement for Canadian citizenship will embolden other countries to impose similar citizenship requirements to bid on their government projects—which, depending on the project, could potentially exclude Canadian citizens. We suggest that Canada instead invoke any citizenship requirements only when required for clearly defined portions of the ETI.

13.5 Data Sovereignty

a) All e-mail servers and data repositories must be housed in Canada.

Comment: We urge governments worldwide to prohibit local infrastructure mandates. Such mandates are discriminatory and contrary to the notion of cross-border trade. Further, national security does not necessarily equate with territoriality of data. For example, facilities in another country (such as the United States) could be more secure than domestic-only ones if the U.S. facilities are built at scale. Finally, such a mandate also could embolden other countries to impose similar requirements, which could be extremely disruptive to global cross-border data flows, affecting a wide range of multinational companies, likely including those based in Canada.

e) In the event of unauthorised access to Canada's data (e.g. access that has not been expressly permitted by Canada) within the Email Solution (e.g. to comply with a foreign government's production order), there will be no limit to the Email Solution provider's liability to Canada for such unauthorised access.

Comment: We are very concerned with a provision of unlimited liability. Liability must be commensurate to some degree with the value of the contract.

13.6 Supply Threats to the Government of Canada

In addition to the threat of cyber attack, there is a growing awareness of the risks posed by potentially vulnerable or shaped technologies that may be entering the GC communications networks and IT infrastructure through the supply chain. The Contractor must provide the GC with a list of all hardware and software manufacturers and vendors proposed to be used in the IT Infrastructure and Services of the ETI in advance of contracting with them. Canada reserves the right to reject a hardware or software manufacturer and/or vendor for security and/or business stability reasons.

Comment: A requirement to name all hardware and software vendors and manufacturers proposed to be used, with the possibility that Canada could reject a manufacturer and/or vendor for "security and/or business stability reasons" is of concern. We fear that such a requirement could lead to exclusion of vendors based on country of origin or the nationality of the technology vendor. The *Global Information and Communications Technology (ICT) Industry Statement: Recommended Government Approaches to Cybersecurity, June 2012*, referenced above, recommends that governments "ensure that cyber security requirements allow for procurement of technologies regardless of the country of origin or the nationality of the technology vendor. Product security is a function of how a product is made, used, and maintained, not by whom or where it is made. Governments should re-examine their understanding of cyber supply chain risk, acknowledge that ICT vendors are best placed to manage and protect their ICT supply chains, and partner with industry on solutions that build bridges rather than exclusionary trade walls."

(ii) The questions provided in Part IV of this RFI

Q04: If Canada was to restrict the provisioning of the Email Solution to a Canadian company, or a Canadian foreign subsidiary (e.g. a Canadian company, operating in Canada, which is a subsidiary of a foreign parent company), and further restrict the use of subcontractors to Canadian companies and Canadian foreign subsidiaries, how would this affect your service offering in still meeting ETI's service requirements?

Comment: We are concerned about this idea for a few key reasons. First, similar to our comments on Canada's claim of the National Security Exception, we fear that if Canada were to place such restrictions on this project (or other projects), it would embolden other governments to similarly restrict the right to bid on projects to domestic companies—harming foreign companies' competitiveness in potentially multiple foreign markets. In addition, a "domestic-company only" approach may end up decreasing, not increasing, security of the Canadian Government. The security of technology and services is not dependent on by whom, or where, the products or services are made. Security is a function of how products or services are produced, procured, and maintained.

Q55: The GC has an objective to minimize the risk of a security or privacy breach due to vendor negligence and due to a vendor being compelled by a foreign nation to hand over email information owned by the Government of Canada. What are your thoughts on unlimited liability to achieve this objective?

Comment: Per our answer to 13.5(e), liability must be commensurate to some degree with the value of the contract. Because most companies' legal counsel likely would not allow a vendor to sign a contract exposing them to unlimited liability, this provision could have the unintended effect of reducing the pool of bidders on this project.

Conclusion

Thank you very much for your consideration. Please consider ITI and its member companies a resource for the Canadian Government on cybersecurity issues moving forward. Do not hesitate to contact us at any time with any questions at dkriz@itic.org.

Sincerely,

Danielle Kriz

Director, Global Cybersecurity Policy