Encryption Alert: New Permit for Exports and Technology Transfers to EU Plus Five Countries

February 3, 2011

by John W. Boscariol (jboscariol@mccarthy.ca, 416-601-7835) & Orlando E. Silva (osilva@mccarthy.ca, 416-601-8028), McCarthy Tétrault LLP, Canada.

On February 2, 2011, Canada's Export Controls Division (ECD) announced the availability of a new multidestination export permit for the export or transfer of information security goods and technology to the countries of the European Union (except Cyprus) and Australia, Japan, New Zealand, Norway and Switzerland.

Canadian exporters of encryption-related items have been facing significant challenges with transfers of these items from Canada and have been expressing concerns regarding the impact of these controls on their competitive position in the international marketplace. In response, ECD has been considering means of facilitating the permit process while still complying with Canada's international commitments in this area.

These consultations are further described in our earlier legal alerts: Canadian Government Launches Consultations on Encryption Controls [http://mccarthy.ca/article_detail.aspx?id=4896] and Canadian Government Undertaking Industry Consultations on Cryptography Export Permit Process [http://mccarthy.ca/article_detail.aspx?id=5067].

Late last year, ECD clarified and announced certain changes to its policy regarding the issuance of permits for cryptographic goods, software and technology. Further information on these guidelines can be found in our alert, Canada Issues New Guidance on Encryption Controls [http://mccarthy.ca/article_detail.aspx?id=5138].

Key Conditions for EU+5 Permit

The new "EU+5" permit appears to be designed to offer some flexibility in the terms and conditions applicable to transfers to the identified countries. The key points are:

(i) it applies to hardware, software, source and object code, and technology that incorporate cryptography controlled in Category 5, Part 2 of Group 1 of the Export Control List, excluding items in 1-5.A.2.a.2 (designed or modified to perform cryptanalytic functions), 1-5.A.2.a.4 (specially designed or modified to reduce the compromising emanations of information-bearing signals), and 1-5.A.2.a.9 (designed or modified to use quantum cryptography);

(ii) it authorizes exports to final consignees in Australia, Austria, Belgium, Bulgaria, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Malta, Netherlands, New Zealand, Norway,

Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, and the United Kingdom;

(iii) it excludes any exports or transfers involving countries on Canada's Area Control List or subject to Canadian economic sanctions; at the present time these are Afghanistan, Belarus, Burma (Myanmar), Congo, Côte d'Ivoire, Cuba, Eritrea, Guinea, Iran, Iraq, Lebanon, Liberia, North Korea, Pakistan, Rwanda, Sierra Leone, Somalia, Sudan, Syria, and Zimbabwe;

(iv) it excludes exports for end-use that is directly or indirectly related to research, development or production of chemical, biological or nuclear weapons, or any missile programmes for such weapons;

(v) it has a validity period of five years and requests to extend the validity of export permits may be made up to three weeks before the expiry date;

(vi) there are no reporting requirements, however, exporters using this permit must retain documentation which demonstrates that the exporter has undertaken due diligence to verify that the transaction complies with the permit terms and conditions; this documentation includes contracts, invoices, requests for products, statements of work, specific correspondence, (if applicable) vendor/reseller/distributor agreements, and bills of lading.

More information on the EU+5 permit can be found on ECD's website here: http://www.international.gc.ca/controls-controles/export-exportation/crypto/eu_5.aspx?lang=eng.

Canadian Encryption Controls

Canada continues to apply broad export and technology transfer controls to information security items. Subject to certain exceptions, all hardware, software and related technology designed or modified to use, work with or perform cryptographic functions (employing a key length in excess of 56 bits) is controlled for export or transfer to any non-US destination.

Failure to comply with these controls can have significant financial and reputational consequences. In many cases when product is detained or seized by the Canada Border Services Agency just prior to export because of compliance uncertainties, the ensuing delays can strain customer relations and result in lost business.

Any businesses that use or transfer encryption should be carefully following developments in this area, not just to ensure that they are in full compliance with the requirements but also that they are using all available mechanisms to maintain or enhance their competitive position internationally.