

Export Controls Alert: Canada Issues New Guidance on Encryption Controls

On October 19, 2010, the Export Controls Division of Foreign Affairs and International Trade Canada (ECD) released new information on its policies regarding the application for and granting of permits for the export or transfer from Canada of information security goods, software and technology. Canada imposes controls on transfers of these items to all countries other than the United States.

In response to significant concerns expressed in the Canadian business community regarding the impact of these controls on their competitive position in the international marketplace, 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](#) and [Canadian Government Undertaking Industry Consultations on Cryptography Export Permit Process](#).

This week, ECD clarified and announced changes to its policy regarding the issuance of permits for cryptographic goods, software and technology. These new guidelines can be found at [Export Permits for Cryptographic Items](#). Among other things, they specify that exporters must now have a comprehensive compliance plan in place regarding the export and transfer of controlled goods and technology.

Below is a summary of the key points in ECD's new guidelines.

(i) Multi-destination Permits Available to Exporters

ECD has identified a number of multi-destination permits that are now available to exporters of cryptographic items. These enable exporters to ship or transfer items to consignees in multiple countries and may offer some flexibility in certain circumstances. They include the following:

- Broadbased permit: for exports of hardware, executable software, and associated information and enhancements to a wide range of countries; requires reporting every six months; applicants to whom export permits have not previously been issued or who have a history of non-compliance will be subject to a shorter validity period;
- Co-development permit: for exports of controlled software, source code and other technology containing cryptographic functionality and related technical data and assistance for product development to affiliates in a wide range of countries; locations of those affiliates must be reported but are not required to be declared at the time of application;
- Bona fide Canadian and US corporations permit: for exports of hardware, executable software, and associated information and enhancements to foreign consignees that are majority-owned by Canadian or US-based parent companies; no reporting requirements;
- Regime decontrol (ancillary cryptography) permit: for exports of any goods or technology that meet the definition of "ancillary" cryptography; no reporting requirements (this is more fully described in our legal alert at [Export Controls Alert: Canada's Response to Liberalization of Controls on Ancillary Encryption](#)).

- Java permit: for exports of hardware and executable software into which the Java Runtime Environment has been integrated, as well as associated information and enhancements, to a wide range of countries; no reporting requirements; and
- Financial institutions permit: for exports of hardware, executable software, and associated information and enhancements to financial institutions in a number of countries that have enacted legislation to counter money laundering; no reporting requirements.

It is important to keep in mind that these are not exemptions or de-controls. In these circumstances, exporters must still apply for and obtain these multi-destination permits prior to exporting or transferring the covered cryptographic items. Experience suggests that this can be a lengthy application process. ECD's document provides additional guidance on the information required in such applications.

(ii) Export Compliance Plan Is Now Required

Although it has always been very strongly recommended that exporters have a comprehensive compliance plan in place, ECD is very clear that any exporter seeking to rely on these more flexible multi-destination permits must have such a plan.

ECD states that this must consist of defined or prescribed processes and procedures to ensure that employees at all levels of a company understand and act in accordance with the letter and spirit of the applicable export requirements under the *Export and Import Permits Act*, the *Customs Act*, and other trade-related legislation, including economic sanctions.

ECD requires that such a plan establish the steps and due diligence process a company follows when planning, marketing, and shipping items included in the *Export Control List* to foreign clients, and should also cover download practices. It must provide for a "defined process to provide a reasonable level of assurance (due diligence) that goods or technology may not be exported to unauthorized or illegitimate end-uses or end-users."

(iii) Application Review Periods

Applications for individual export permits (i.e., for the export to specified consignees in a single country) for cryptographic items in respect of many destination countries, including most European countries, Japan, South Korea, Australia and New Zealand, will be reviewed within ten business days from the submission of a complete application. For exports or transfers to other destinations, that period is extended to eight weeks.

Applications for multi-destination permits will be reviewed within eight weeks of submission of a complete application.

(iv) Extended Validity Periods

Individual export permits for cryptography are usually valid for two years. Exporters may request a longer validity periods of up to five years. Individual applications may also be made to extend the validity period of existing permits by up to one year at a time.

The default validity period for multi-destination export permits for cryptography is typically two years, and exporters may request a longer validity period of up to five years. ECD notes that applicants whose product development cycles are shorter than two years may wish to request shorter validity periods since a new application will be required for new versions of a cryptography item.

Canada's Encryption Controls

Encryption controls continue to be a challenge for many Canadian businesses. Failure to comply 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.

Further, 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.

McCarthy Tétrault's International Trade and Investment Law Group has significant expertise in encryption controls, and regularly assists clients in developing solutions to compliance and enforcement issues in this area. We are available to advise on these or any other export control, economic sanction or trade matters. Please feel free to contact any of our partners below:

Contacts

Toronto

John W. Boscariol
416-601-7835
jboscariol@mccarthy.ca

Orlando E. Silva
416-601-8028
osilva@mccarthy.ca

Ottawa

Brenda C. Swick
613-238-2135
bswick@mccarthy.ca

Montréal

Simon V. Potter
514-397-4268
spotter@mccarthy.ca