

## Export Control Issues for Companies Using Encryption Software

---

February 2011

U.S. companies and persons may be subject to export controls in cases when they send, license or transmit encryption software or other related technologies to foreign countries or persons, even if to their own affiliates. Category 5, Part 2 of the Bureau of Industry and Security's (BIS) Commerce Control List (CCL) sets forth these restrictions. Violations of these restrictions can lead to civil and even criminal penalties. It is important to know these restrictions in advance, which can be generally summarized as follows:

- Products with limited use of encryption
  - Some products use encryption in a limited capacity (e.g., authentication or digital signature, execution of copy protected software, and finance specific products designed and limited for banking use or money transactions).
  - Generally, these products have low U.S. export control restrictions.
- Strong encryption products
  - May require review by BIS and approval as Mass-Market encryption products, Unrestricted encryption products, or as Restricted encryption products.
  - Restricted encryption products.
    - May be exported to any end-user (government or non-government) in the EU member countries and other strategic partner countries.
    - In addition, may be export to any non-governmental end-user in all destinations, except U.S. sanctioned countries.
  - Government End-Users are defined as:
    - Any foreign central, regional or local government department, agency, or other entity performing government functions, including governmental research institutions, governmental corporations or their separate business units... which are engaged in the manufacture or distribution of items or services controlled on the Wassenaar Munitions List, and international governmental organizations.
    - This term does not include the following public entities: utilities (including telecommunications companies and Internet service providers); banks and financial institutions; transportation; broadcast or entertainment; educational organizations; civil health and medical organizations; retail or wholesale firms and manufacturing or industrial entities not engaged in the manufacture or distribution of items or services controlled on the Wassenaar Munitions List.
- Products that do not have the primary function of information security, computing, communications, storing information or networking, and the cryptographic functionality is limited to supporting such primary function, can fall outside the scope of Category 5, Part 2.
  - Therefore such products would have significantly less U.S. export restrictions.
  - For example, business process automation, process planning and scheduling, supply chain management, inventory and delivery software utilizing encryption technology can fall outside the scope of Category 5, Part 2 of the CCL.

## Continued

---

- Products that fall within the scope of Category 5, Part 2 of the CCL, may be subject to certain encryption registration, classification, or post-export reporting obligations under the Export Administration Regulations (“EAR”).
- Generally, products with limited use of encryption may be self-classified and do not require encryption registration or post-export reporting.
- Other products may be self-classified, but require encryption registration with BIS to receive an Encryption Registration Number (ERN).
- For some products, the exporter may be required to file an annual self-classification report to BIS.
- If encryption registration is required, and self-classification is not applicable, then the filing of an encryption classification request is necessary. Generally, this applies to strong encryption products and often requires a semi-annual report to be filed to BIS.

Joseph Gustavus  
**+1.248.267.3317**

Jeffrey Richardson  
+1.248.267.3366