WILMERHALE

New Encryption Export Regulations May Be Changed Again Soon

2000-06-01

Barely six months after the latest restructuring of encryption export control regulations, another major change may already be on the way.

For years, the U.S government strictly regulated exports of cryptographic hardware, software, components, and technology. The U.S. insisted that widely available data-scrambling technologies could endanger national security, notwithstanding the fact that comparable encryption products were readily available from foreign producers under the weaker export control policies of most other industrialized countries. Then, in September 1999, the U.S. conceded that the rules were out of step with the global but security-conscious Internet economy; a new set of export regulations was unveiled in January 2000.

U.S. Moves Toward International Consensus. Now, in a significant policy shift, the U.S. official in charge of encryption export controls says that the U.S. will relax its encryption rules yet again if, as expected, the European Union further weakens its encryption export controls. Commerce Department Undersecretary William Reinsch told a recent high-tech conference that U.S. encryption export controls will be liberalized as necessary to maintain the competitiveness of U.S. companies in the burgeoning global market for computer and network security products and services. Export officials had previously maintained that U.S. policy would not be driven by decisions of foreign governments.

Revised Rules Are More Permissive, Still Complex. For the time being, however, U.S. exporters must observe the confusing patchwork of encryption export regulations as they were reformulated in January 2000. Under these rules, most new commercial encryption products may not be exported until they are reviewed by the Commerce Department and a panel of other federal agencies. In addition, many encryption exporters are required to file post-shipment sales reports with the Commerce Department. Although encryption items are more easily exported, the regulatory system is as confusing and as peppered with narrow exceptions as it was in the past. Highlights of the January 2000 encryption export rules are summarized below. The complete rules are posted on the Commerce Department's website, and should be consulted before attempting to export any encryption item.

Non-Government, End Users . After a one-time review, encryption products of any strength are exportable to non-governmental end users worldwide, except for the "terrorist" and embargoed countries (currently, Cuba, Iran, Iraq, Libya, North Korea, Serbia, Sudan, Syria, and Taliban-controlled areas of Afghanistan). It is generally no longer necessary to follow separate export procedures based on encryption key length, a product's "recoverability," or the type of end-user or end use. Products which have been reviewed in the past may be exported to non-governmental foreign end users without a new technical review, unless the prior authorization allowed exports only to subsidiaries of U.S. companies.

"30-Day" Technical Reviews. According to the regulations, technical reviews of encryption products are supposed to be completed within 30 days. In practice, however, these reviews may take two months or more from the date of filing. If the Commerce Department fails to respond to a review request within 30 days, then most encryption items may be exported anyway to non-governmental foreign end users, subject to reporting requirements.

"Retail" Encryption Items . If the government determines that an encryption product is a "retail" product, then it may be exported to any end user, including foreign government end users, except in the prohibited countries. "Retail" products are those which (1) are designed for individual consumer use, or sold through independent retailers; or sold to the public in large volume via telephone, mail order, or electronic transactions; and (2) do not require substantial technical support for installation and use; and (3) do not allow users to easily change the encryption functionality; and (4) are not customized to a customer's specifications; and (5) are not "high-volume" network infrastructure products. "Retail" certification requires a special ruling from the Commerce Department, except that previously reviewed 56-bit products and qualifying "finance-specific" products may be considered to be "retail" encryption products without additional review.

Telecommunications and Internet Service Providers . Export licenses are still required for exports of non-"retail" encryption products to Internet and telecommunications service providers if the products are used to provide services specifically to foreign government customers.

Commercial Encryption Source Code and Toolkits. Encryption source code which is "publicly available" may be exported without prior review. However, if the source code is subject to a licensing fee or royalty for the right to use the code in a commercial product, then the exporter is required to notify and disclose the code to the government "by the time of the export." Encryption source code which is not publicly available and general-purpose encryption "toolkits" may be exported to non-governmental end users after a one-time review. Export licenses are still required for "open cryptographic interfaces" which do not contain encryption, but which facilitate the insertion of encryption capabilities without assistance from the manufacturer.

Subsidiaries of U.S. Companies. Encryption items of any strength may be exported to foreign subsidiaries of U.S. companies, including their foreign employees, without any prior review or licensing. However, new products developed from the exported products are still subject to one-time review before they may be released outside of the company.

Key Length Upgrades . Any "mass market" encryption product previously reviewed and authorized

for export may be upgraded to 64-bit encryption without a new technical review, provided the exporter certifies to the Government that the encryption is unchanged except for the increased key length.

Reporting Requirements. Semi-annual post-export reporting is required for most commercial encryption exports. However, reporting is not required for (1) products with key lengths of 64 bits or less; (2) products limited to encryption of specific financial data; (3) "retail" products exported to individual consumers; (4) products which are distributed for free or by anonymous download; (5) products exported to foreign subsidiaries of U.S. companies; or (6) products exported to subsidiaries, affiliates, customers or contractors of a U.S. bank or financial institution.

Internet Exports. Encryption software may still be "exported" when it is downloaded from the Internet. Accordingly, encryption-enabled software should not be posted on the Internet without ensuring that any required reviews and approvals have been obtained. For non-"retail" encryption software which cannot be exported to foreign governments without an export license, the regulations require online screening procedures to ensure that the requestor is not located in a prohibited country and that the intended user is not a foreign government organization.

"Deemed Exports." U.S. export controls generally apply to disclosures of controlled technologies or software to foreign persons in the U.S. (such as H-1B visa holders). Such disclosures are called "deemed exports." Special deemed export rules apply to encryption items.

- Encryption object code and source code is not considered to be "exported" when it is disclosed to a foreign person (other than a representative of a foreign government) in the U.S.

- Encryption-related technology, technical data, and know-how (as distinguished from object code or source code) may be disclosed to foreign individuals from non-prohibited countries who are working in the U.S. for U.S. companies. However, an export license is still needed prior to disclosing encryption technology to foreign employees of foreign companies who are working in the U.S.

Conclusion. The rules governing encryption exports remain in a state of transition and exporters are expected to comply with the very latest Commerce Department instructions. Accordingly, it is important to plan ahead before exporting any encryption-enabled hardware, software, components, or technology in order to leave time for the one-time technical review which remains a prerequisite for most encryption exports. If the past is any guide, future "liberalization" of U.S. encryption export policy does not necessarily mean "simplification."

Authors

Barry J. Hurewitz

PARTNER

barry.hurewitz@wilmerhale.com

+1 202 663 6089