Posted: November 29, 2011

INTANGIBLE EXPORTS (EXPORTS OF TECHNICAL INFORMATION)

TABLE OF CONTENTS:

1.0 PURPOSE

The development and implementation of internal controls over intangible exports should be one of the top priorities of any organization involved in export-controlled activities. Technical information may be considered more sensitive than tangible goods because it can be used in the design, development, production and manufacture of goods. Because of the sensitivity of the technical information associated with intangible exports, and the inherent difficulty of meeting the very broad regulatory requirements associated with these exports, export enforcement authorities place a high priority on investigating transfers of technical information. Because of the growing awareness of the sensitivity of intangible exports, both from a national security and a commercial/proprietary perspective, these exports are increasingly governed by a patchwork of export control standards across a number of different countries and regulatory regimes.

Technical information often moves multiple times and in multiple directions, with each cross-border transfer of information potentially implicating the trade controls of the countries of export, import and/or origin. Accordingly, procedures for the control of intangible exports should not just establish controls on the development and initial transfer of technical information outside its country of origin but also controls on potential additional movements of that data, including transfers to third countries as well as transfers back to the original source country

For these reasons, it is vital that exporters maintain strict internal controls over intangible exports, both in order to meet the regulatory requirements associated with these exports, and to demonstrate due care in the event of any inadvertent violation of these regulatory requirements.

2.0 REQUIREMENTS[1]

2.1 General

2.1.1 Personnel responsible for ensuring compliance with export control laws and regulations must have the authority within the organization to stop to any transfer of technical information which would violate export control laws and regulations.

[1] Organizations should also ensure that any data contained on these devices is protected in accordance with their internal procedures for protection of information, as the data may be subject to inspection by foreign or domestic Customs officials or could be stolen while on travel. Organizations should consider implementing the technical suggestions published by the U.S. National Security Agency for securing laptops, personal mobile devices, and home networks, and for using social networking sites, at: http://www.nsa.gov/ia/_files/factsheets/Best_Practices_Datasheets.pdf.

2.1.2 Organizations should have a system for tagging, marking, or otherwise identifying electronic files containing export-controlled technical information before those files are released outside of the domestic organization or otherwise made available to foreign persons.

2.1.3 Organizations should provide regular training to all employees who interact with foreign persons on the requirements of export control laws and regulations pertaining to intangible exports.

2.1.4 Export Exceptions/Exemptions

- Although export control regimes may offer broad exceptions/exemptions covering many situations where intangible exports would otherwise require a license, these exceptions/exemptions are subject to a number of conditions and requirements that must be satisfied in order for the exceptions/exemptions to be properly used.
- Organizations should have a process in place to verify any such authorizations and to document the use of any exceptions/exemptions before the intangible export activity takes place.

2.1.5 Organizations should ensure that all export activities related to intangible exports are audited for compliance with the applicable regulatory requirements on a regular basis.

2.2 Hardware Containing Technical Information

2.2.1 Screening Hardware Exports

- Exporters must have an internal control system for confirming that all laptops, PDAs, thumb drives, servers, backup tapes, test or diagnostic equipment, or any other hardware containing technical data, being exported have been screened for possible export-controlled technical information.
- This screening should include both potential export controls on the software that is pre-loaded onto the device (including off-the-shelf disk encryption[2] or anti-virus software), as well as any export controls on technical information that has been loaded onto the device by the user.

2.2.2 Organizations should have a process in place to ensure that employees obtain authorization prior to travelling to a foreign destination with a laptop or other electronic device that contains controlled data or software. In cases where it is not practical to determine whether the employee's device contains controlled data or software, organizations should encourage employees to travel with a "sanitized" device. A "sanitized" device should not contain any documents, presentations, or other controlled information other than a standard set of pre-loaded software that has been approved by an organization's export compliance personnel. An organization should also have a standard process in place for reviewing any additional data or software loaded onto the "sanitized" device by the user.

2.2.3 Organizations should have a procedure to ensure that devices containing controlled technical data are sanitized before disposal, scrap, sale, return at the end of the lease, etc. This could include photocopy machines.

2.2.4 Individuals involved in exporting a device containing controlled data or software should be briefed on the export control requirements associated with intangible exports. Organizations should also have a trip-specific process in place to address any country-specific export compliance requirements associated with the files being exported on the device.

[2] In addition to export authorization, the organization may be required to obtain import authorization from the destination country.

2.3 Electronic Transfers of Technical Information

2.3.1 Organizations should follow one of the two following options for managing electronic access to export-controlled technical information: 1) maintain a system of access restrictions for the servers and information systems that contain controlled data, and grant access to users and IT support personnel at the system-level and server-level; 2) maintain a system of access restrictions for each item of technical information that requires an authorization and grant access to users and IT support personnel at the data-level. Regardless of which method is chosen, all systems for controlling access to export-controlled information should include restrictions on any information systems that are accessed by persons and/or destinations requiring export authorization (including employees, agents, consultants, contractors, visitors, and the general public), including, but not limited to:

- Electronic files transferred via email;
- Network services and information systems managed via a "cloud computing" service, remote server farm, logistics database, etc.;
- Distribution of export-controlled software or technical information via the internet or other electronic means;
- Electronic files made available via the organization intranet;
- Servers used to store and manage access to product data such as design specifications, manufacturing routers, or other detailed product information;
- Discussion rooms or other collaboration sites used by engineering teams in separate locations; or
- Video/audio conference feeds used for meetings between different engineering/product teams.

2.3.2 This system for controlling access to electronic files containing export controlled technical information should have a documentation process in place that includes the party to whom access is being provided, the person granting access to that party, the date access is being granted, and a confirmation that an appropriate, authorized export control employee has approved that party for access to the technical information at issue.

2.3.3 In cases where a foreign person is permitted, under a valid export authorization, to access electronic files containing export-controlled technical information, the organization should have a system in place to ensure the following:

- That all applicable individuals (including any foreign recipient(s) to whom the information is being provided, the supervisor of any recipient(s), and any person who would be called upon to provide export-controlled technical information to the recipient(s)) have been advised of the limitations of this access and on any retransfer restrictions that apply to this technical information;
- That the foreign person does not have access to any technical information which is outside the scope of the applicable export authorization; and
- That all access to the system, and to the individual files in that system, by the foreign person is fully documented in accordance with the requirements of the export authorization and/or the applicable regulatory requirements.

2.3.5 Organizations should be aware of the particular controls that apply to export-authorized persons who are actively downloading[3] export-controlled technical information while physically located in a country that is not included on the applicable export authorization, and should implement appropriate controls to ensure that any such file transfers are covered under an applicable export authorization, and that any

[3] This proposed best practice does not address an export-authorized person who is only visually accessing, and not downloading or printing, export-controlled technical information while physically located in a country that is not included on the applicable export authorization. Whether visual access alone is considered an export in this scenario varies from country to country.

conditions or requirements on that authorization (including all documentation requirements) are met prior to permitting such download access.

2.4 Oral/Visual Transfers of Technical Information

2.4.1 Organizations should implement internal controls to ensure that any interaction with foreign persons (whether in-person or via telephone/video conference) that may involve the verbal/visual transfer of technical information is screened by trained personnel for potential export control issues prior to the interaction, and that any concerns are immediately reported to the organization's export control authorities for resolution.

2.4.2 In cases where an oral/visual transfer of export-controlled technical information is authorized under a valid export authorization, organizations must have controls in place to ensure the following:

- That the party providing the technical information has been advised of the limitations of the export authorization under which the oral transfer is taking place;
- That all parties receiving the technical information understand any retransfer restrictions required by the export authorization; and
- That the oral transfer has been fully documented in accordance with the requirements of the export authorization and/or the applicable regulatory requirements.