Policy on Electronic Transfers of Technology Including Access Abroad

Introduction

Electronic transfers of technology (often referred to as technical data) may occur when an e-mail is sent, access to a platform is granted, during a Web-ex, video conference etc. If the technology is subject to export control, and the recipient is abroad, of a different nationality or employed by a different company, there will be export control implications associated with such activities

There will also be export control implications if controlled technology is stored on a server in a foreign country. The location of help desks and remote administrators for either domestically based or foreign based servers may give rise to export control concerns if the help desks and administrators are able to gain access to export controlled technology stored on those servers.

Similarly, when individuals travel abroad with export controlled technology on their electronic devices, or while abroad they use an electronic device to access export controlled technology remotely, an export will have occurred.

It should be noted that common ownership does not preclude the application of export controls. For example, when technology is sent from Rolls-Royce in the UK to Rolls-Royce North America, if that technology is subject to control, it will require an export license or authorisation, even though both parties are effectively within the same company.

Governments' export control policies associated with electronic transfers of technology are still developing. In some instances they lack clarity and certain actions do not appear to be addressed at all in published guidance. For instance, information on the need for an authorisation from a country visited when an individual leaves to return home, or to travel from there to another foreign country, with export controlled technology stored on their electronic device, is rarely covered.

Policy

1. Each Rolls-Royce business, whether wholly-owned or JV, or function must classify, record and manage export control classification data for all technology. (See policy on Product and Technology Classification.)
2. It is essential that businesses and functions address the export control implications of sharing technology via electronic means and ensure that authorisations are in place to permit:-

(a) The sharing of export controlled technology with others based abroad, whether they are part of Rolls-Royce or from an outside concern;

(b) The sharing of US export controlled technical data that may, for instance, be stored on shared network folders or on a platform with 3rd parties (e.g. suppliers, contractors, engineering services organisations and consultants whether at home or abroad);

(c) The sharing of US export controlled technical data in the US with other employees who are foreign nationals;

(d) The storage of export controlled data on servers based abroad and the activities of help desks and remote administrators based abroad;

(e) The export of technology on electronic devices by individuals and access to technology remotely while abroad.

3. It is the responsibility of businesses and functions, working closely with the IT and export control functions, to ensure that individuals are aware of the server location of the databases and data sharing applications used, and the export authorisations in place for those servers, so that individuals do not inadvertently commit export control violations through a lack of awareness.

4. Individuals in businesses and functions must ensure that they do not send export controlled technology to any individual in Rolls-Royce, or to an outside concern, before determining where they are based. Any transfer abroad must be covered by an appropriate export authorisation and the individual is also responsible for maintaining appropriate records of transfers that take place (see policy on Record Keeping).

5. When an individual proposes to take IT equipment abroad they should download the appropriate IT Equipment Permit ('Border Card' or 'Export Control Coversheet' in the US). Where the form requires either the signature of an approved export point of contact (EPOC) or export control manager this must be obtained prior to travel. These only permit exports of technology specified and access by the individual named to the destinations specified. They provide notification to Customs of the type of technology/data held on the equipment, or that will be accessed remotely while overseas, and the export license or authorisation covering it where one is needed.

6. If an individual is intending to provide any technology or documents to a customer, supplier or other third party while overseas they should first consult their local EPOC or export control manager (a specific export licence, non-disclosure agreement or intellectual property licence may be required).

7. Before setting out on a trip with controlled technology on an electronic device, individuals should consult their local EPOC or export control manager and IT Security about risks associated with leaving the country visited with such technology still on

their device. In cases of doubt individuals should delete any export controlled technology or links to accessing such technology prior to departure or arrange for an approved form of data cleansing.

8. In addition to export control an individual needs to consider the associated Travel Security controls which include high risk destinations, IT Security and Intellectual Property control requirements.