**Cloud Computing Best Practices**[[1]](#endnote-1)

If your enterprise stores data or information “in the cloud,”[[2]](#endnote-2) you should determine if any of the data is subject to strategic trade control. In some jurisdictions, if controlled data is stored or routed outside of the country, or shared with foreign nationals, it is deemed to be an export and requires authorization from the national authorities. **Your enterprise should consult with the national licensing authorities to address the following questions:**

1. When is technology or software said to be “exported” or “transferred”?
2. Is data stored abroad in the cloud considered an “export” to the foreign country?

**If applicable, your enterprise can take the following actions to minimize the possibility that controlled data or information stored “in the cloud” is accessed by unauthorized end-users:**

* Determine the physical routing and destination of any controlled technical data that has been uploaded to the cloud in order to determine whether licensing requirements apply (Where does the data reside? Where are the servers located?);
* Seek assurances from providers that any controlled data will be located entirely on local servers in your country, and that it will not be accessed by foreign nationals employed by the providers;
* Even with commitments from providers, your enterprise should continue to exercise due diligence to monitor when controlled data is maintained or routed, outside of your country or made accessible to foreign nationals;
* When unsure of the implications of a cloud service arrangement, seek guidance from the national authorities to determine whether a license is required to transfer controlled data from the cloud;
* Impose restrictions on creation of copies of data by cloud service providers, and require that providers delete all copies (including backups) of such data once cloud services are terminated;
* Review and modify internal compliance policies and practices, (and TCP, if applicable),
* Inform and update employees on any emerging compliance issues related to the cloud;
* Ensure that cloud service agreements address each party’s compliance responsibilities, and the penalties and consequences for acts of noncompliance; and
* Increase the security of your data by adding passwords, logins, and/or encryption to access.

1. Adapted and modified from “Impact of Export Controls on Higher Education & Scientific Institutions,” Georgia Tech University, May 5-7, 2014. [↑](#endnote-ref-1)
2. **Definition:** “Cloud computing” is a distributed computing environment orchestrated over a network. See, “Impact of Export Controls on Higher Education & Scientific Institutions,” Georgia Tech University, May 5-7, 2014, <http://researchintegrity.gatech.edu/files/Export/2014-conference-presentations/Cloud\_Computing\_and\_Encryption\_Cowperthwait\_Metcalf\_Schlesinger\_Smoak\_Wheeler.pdf>. [↑](#endnote-ref-2)