Limiting export controls on encrypted cloud data: a tiny umbrella in a big storm

Proposed rules from BIS and DDTC seek to bring regulation of cloud-based services up to date and in keeping with current technological norms and business practices. Joseph Schoorl examines the two proposed rules and their individual and collective impact for both cloud users and cloud service providers.

On 3 June 2015, both the U.S. Commerce Department’s Bureau of Industry and Security (BIS) and the U.S. State Department’s Directorate of Defense Trade Controls (DDTC) issued complementary rules (collectively, the ‘Proposed Rules’) that, if enacted, would represent an important albeit small step toward modernising U.S. export controls to better address modern technologies, in particular, cloud-based services and intangible technology transfers. These Proposed Rules were issued as part of the broader Export Control Reform initiative that has been ongoing since 2009. BIS and DDTC provided a 60-day public comment period ending on 3 August 2015, and the agencies will be reviewing these comments before issuing final rules.

If implemented in their current form, the Proposed Rules would revise a number of fundamental definitions in the Export Administration Regulations, 15 C.F.R. Parts 730-774 (‘EAR’), and the International Traffic in Arms Regulations, 22 C.F.R. Parts 120-130 (‘ITAR’), respectively. These Proposed Rules include important new provisions that are directly relevant to users of cloud-based services. In particular, the Proposed Rules would exclude transfers of encrypted technology, technical data, or software from the definitions of exports or re-exports so long as certain requirements are met. While these encrypted data carve-outs reflect a welcome step toward adjusting U.S. export controls to match the national security risks presented by cloud computing, companies should be aware that the requirements for relying on these carve-outs will significantly limit their application. In fact, the Proposed Rules would not eliminate export control compliance concerns regarding cloud computing so much as create additional compliance provisions requiring consideration as part of a broader technology control plan.

**Background**

For years, the question of how to use cloud-based services in a manner that complies with U.S. export control regulations — and who is responsible for such compliance — has attracted a great deal of attention within the export control compliance community. Because ‘the cloud’ is composed of physical servers that can be located around the world, cloud users storing or accessing controlled technology, monitoring and screening activities would not be considered to have received a deemed export or deemed re-export under the EAR. Finally, in a November 2014 opinion, BIS advised that no exportation or re-exportation of software occurs if a cloud-based storefront allows customers to utilise

28 WorldEPR www.worldecr.com
applications stored on servers without downloading the application itself to a local machine. DDTC has not provided any comparable public guidance about these broad questions.

While helpful in providing guidance about BIS's approach to cloud computing and laying out the expectations that apply to cloud service providers, these advisory opinions notably failed to address the compliance risks that would be faced by cloud users. This uncertainty has led many users of cloud-based services to assume the broaderest possible application of the EAR and ITAR to the cloud. As such, the transmission or storage of controlled technology, technical data, or software on the cloud is regularly treated as an 'export', regardless of whether this transmission or storage affects the ability of parties in other countries to access this data. This has resulted in many users favoring domestic and/or 'private clouds', which are often more expensive, or avoiding the cloud altogether. The Proposed Rules are a welcome development because they directly address the unique regulatory issues presented by using cloud services in connection with controlled technology, technical data, or software.

**Summary of the proposed cloud-related provisions**

Building on a proposal made by the Defense Trade Advisory Group in May 2013, both Proposed Rules include provisions that essentially exclude from the definitions of 'export' and 're-export' all transfers of encrypted technology, technical data, or software that meet certain specific requirements. This proposed policy reflects the reality that, as BIS states, information that is protected by sufficient encryption is 'useless to unauthorized parties unless and until it is decrypted'. Accordingly, BIS explains that any transfer of such encrypted information 'poses no threat to national security or other reasons for control and does not constitute an "actual" transmission of "technology" or "software". This distinction between encrypted information and "clear text" information — i.e., information in a form that is readable by humans or machines — is essential for both Proposed Rules, and it reflects a much-needed consideration of how the circumstances in which cloud computing services could jeopardize the national security goals of the U.S. export control regimes.

Both Proposed Rules provide similar (though not identical) requirements that must be met in order for the respective encrypted data carve-outs to apply. These requirements are as follows:

1. **The information must be unclassified**
   The Proposed Rules' respective carve-outs for encrypted data would apply only to technology, technical data, or software that is not classified national security information.

2. **The information must be protected by end-to-end encryption**
   Importantly, the encrypted data carve-outs would only be available for technology, technical data, or software that is secured by so-called 'end-to-end' encryption. Both Proposed Rules define end-to-end encryption as providing 'uninterrupted cryptographic protection of data between an originator and an intended recipient'. The Proposed Rules go on to explain that the end-to-end encryption requirement would not be met if, at any stage in its transmission or storage, the data would be viewable in unencrypted form by third parties such as internet service providers and cloud service providers.

3. **The encryption must meet specific encryption standards**
   The Proposed Rules set out minimum requirements for the level of encryption that must be utilised before transmitting or storing data to qualify for the encrypted data carve-outs. The DDTC Proposed Rule would require that technical data or software be secured using cryptographic modules compliant with the Federal Information Processing Standards Publication 140-2 (FIPS 140-2) and supplemented by software implementation, cryptographic key management, and other procedures and controls that comply with guidance in the U.S. National Institute for Standards and Technology publications. The BIS Proposed Rule provides for greater flexibility by allowing the use of those same standards or of 'similarly effective cryptographic means'.

4. **The encrypted information must not be stored in certain countries**
   Even if the above requirements are met, the Proposed Rules provide that the encrypted data carve-outs would not apply for data stored in Russia or in countries that are subject to US arms embargoes.

Because this new policy hinges on the protection that encryption provides, both Proposed Rules also include revisions that would impose new controls on releases or transfers of encryption keys, passwords, and other information (collectively, 'Access Information') necessary to decrypt or otherwise access encrypted data. The BIS and DDTC approaches to Access Information are slightly different, however. Under the BIS Proposed

---

**Links and notes**

6. BIS Proposed Rule, 35109.
7. 1d.
8. DDTC Proposed Rule, 35137; BIS Proposed Rule, 35127.
9. Countries subject to US arms embargoes are listed in Country Group G.S in Supplement No. 1 to EAR § 740.1 and in ITAR § 126.1.
10. BIS Proposed Rule, 35161.
11. DDTC Proposed Rule, 35135.
13. BIS Proposed Rule, 35159.
14. DDTC Proposed Rule, 35129.
Rule, releases of Access Information would be exports or re-exports only if the releasing party has knowledge (or reason to know) that this release would cause or permit the transfer of clear text technology or software to a non-U.S. national. By contrast, the DDTC Proposed Rule would consider releases or transfers of Access Information to be exports or re-exports regardless of whether technical data or software is actually accessed. For purposes of determining whether a licence was required and a violation occurred, both of the Proposed Rules would treat the export or re-export of the Access Information itself as an export or re-export of the underlying technology, technical data, or software that is secured using that Access Information.

Meeting the end-to-end encryption requirement

Of all the provisions in the Proposed Rules' carve-outs for encrypted data, the end-to-end encryption requirement represents the most significant limitation on the scope of those carve-outs. Users have come to rely on cloud computing for a large number of services other than data storage and transmission, including not only some types of webmail but also applications that only recently migrated from the desktop to the web browser (e.g., word processors, spreadsheet applications, data analysis tools). In order to function, these 'Software as a Service' or 'SaaS' products generally require access to clear text data uploaded or input by users. This functional requirement of SaaS makes these products less likely to meet the end-to-end encryption requirement — a fact admitted by BIS in the BIS Proposed Rule.

Of course, even cloud providers that do not market SaaS products might not implement true end-to-end encryption because of the complexity of these implementations and the potential burdens they place on users. Importantly, these providers may advertise that the use of their services is protected by encryption. If this statement is only referring to encryption measures that protect against access by outside parties and does not apply to access by the cloud provider's own employees, however, uploading unencrypted controlled technology, technical data, or software to such a provider would be outside of the respective scopes of the proposed encrypted data carve-outs.

Ensuring compliance for private clouds

Companies that maintain their own cloud resources (i.e., a 'private cloud') will also need to consider whether their systems meet the requirements for the encrypted data carve-out, and this may prove difficult. Although the language in the Proposed Rules seems mostly applicable to cloud services that are provided by third parties (i.e., 'public clouds'), it is without question that the encrypted data carve-out would also be available for data on private clouds. This could be significant for companies that maintain servers in multiple jurisdictions and wish to allow the flow of controlled information between these servers for purposes of increasing performance or providing redundancy.

It is unclear, however, how the references to 'third party' access in the Proposed Rules' definitions of end-to-end encryption would apply in the private cloud context. If a company's internal network encrypts and decrypts data at multiple points between transmission and storage, this would not fit within the letter of the end-to-end encryption requirement. This structure seems to be less of a national security concern than in the public cloud context, though, if the only 'third party' in a position to view unencrypted information on a private cloud would be the company's IT professionals. Assuming the technology, technical data, or software would remain within the company's secured environment and would not be susceptible to unauthorised access by external parties, this could arguably result in a level of security that is functionally equivalent to the end-to-end encryption requirement.

Protecting Access Information

If the Proposed Rules go into effect as currently drafted, companies using cloud services would also need to consider what Access Information to protect and how to protect it. As explained above, Access Information under the Proposed Rules is essentially subject to the same controls that would apply to the underlying technology, technical data, or software that is secured using that Access Information. This could result in somewhat unique scenarios where a password providing access to a large database of EAR-controlled technology could be treated as controlled under multiple export control classification numbers and thus subject to multiple reasons for control.

Even more problematic would be an encryption key used to secure both ITAR-controlled technical data and EAR-controlled technology because of the ITAR's stricter approach to determining whether a release of Access Information is treated as an...
Cloud users should not overestimate the practical impact that these Proposed Rules would have if implemented. 

The author would like to thank Alison Stafford Powell and Alexandre Larriol for their contributions to this article.