May 16, 2013: Final White Paper

DTAG Cloud Computing Working Group

Working Group Members:

Marjorie Alquist, Working Group Co-Chair, LORD Corporation
Rebecca Conover, Working Group Co-Chair, Intel Corporation

- Lisa Bencivenga, Lisa Bencivenga LLC
- Greg Bourn, Bourn Identity Inc.
- Dennis Burnett, Dennis J. Burnett, LLC
- Ginger Carney, Global Connections
- Michael Cormaney, Luks Cormaney LLP
- Andrea Dynes, General Dynamics Corp.
- Larry Fink, SAIC
- Alfred Furrs, Johns Hopkins University, APL
- Beth Mersch, Northrop Grumman Corporation
- Sam Sevier
- Bill Wade, L-3 Communications
- Dana Goodwin, TradeLink Systems, Inc.
- Greg Hill, DRS Technologies, Inc.
- Spence Leslie, Pentair
- Christine McGinn, InterGlobal Trade Consulting, Inc.
- Terry Otis, Otis Associates, LLC
- Joy Robins, Wind River Systems
- Bill Schneider, International Planning Services, Inc.
- Sal Manno, Inmarsat, Inc.
- Kim DePew, GE Aviation

DTAG Tasking

Cloud Computing: The use of the "cloud" method for data storage creates some significant regulatory challenges for exporters and the U.S. Government.

The Working Group should ***review on use of this data storage method***, its ***various implementation arrangements***, and a report on the ***implications for regulators*** and ***possible guidance that might be promulgated for use by exporters consistent with regulatory controls***.

Background/Definition

Cloud Computing is a service that offers use of software (applications) and infrastructure (such as data centers, servers, routers, storage media, etc.) for creation, collection, processing, storing, maintenance, use, sharing, transmission, dissemination, or disposition of information. Because the cloud can take several forms, the DTAG employed the U.S. Department of Commerce National Institute of Standards and Technology (NIST) definition of Cloud Computing in NIST SP 800-145, "Definition of Cloud Computing." Technical data (as defined in ITAR 120.10) is one of the types of information that can be created, collected, processed, stored, maintained, used, shared, transmitted, disseminated or disposed of in a cloud. Cloud service providers rely on shared and distributed resources to maximize efficiencies and economies of scale. These resources may be distributed over many nations and many time zones but this distribution of resources is not transparent to the user. When the grid is reaching maximum capacity, the ability to move information to avoid overload is critical.

A user of cloud services can have easy access to a large range of services from an information system infrastructure that appears to be dedicated to the user but is in fact shared by many users. The benefits of cloud computing are that all of the services that could otherwise be provided from an enterprise network that incurs both a large capital investment and a high maintenance cost, can be obtained from much larger, resource-rich and redundant virtual networks, whose costs are spread out over many users.

The term *cloud computing* appears to derive from the practice of using drawings of stylized clouds to denote networks in diagrams of systems. The use of the term *cloud* is used as a metaphor for the Internet, based on the standardized use of a cloud-like shape to denote a network.

The use of the term "cloud computing" and thus the "cloud symbol" began to be used to denote the portion of an information system for which the provider was responsible vs. the portion of an information system for which the users were responsible. The boundary between a user and the cloud depends on the circumstance. For example, the boundary of the cloud can start at the wireless interface to a cellular network of a handheld device or start at an enterprise network interface to the world-wide-web.

DTAG Assignment

Cloud Computing: The use of the "cloud" method for storage of technical data creates some significant regulatory challenges for those who use the cloud to create, collect, process, store, maintain, use, share, transmit, disseminate, or dispose of "technical data". Consequently, such use of a cloud also creates some significant regulatory issues for the U.S. Government. While the focus of the DTAG Working Group primarily has been on the use of a cloud for storage, the Working Group has also considered the legal and regulatory implications of the movement (e.g., transmission) of technical data to, within and from a cloud. The DTAG Working Group did not include the issues related to outsourcing of enterprise information systems in its scope but noted that many of the issues raised by cloud computing are implicated in the use of outsourced IT services.

1) Review on use of Cloud as storage method

a. DTAG concluded that the risks to national security and foreign policy of unauthorized export of technical data have increased in near lock step with the exponential technical advances in computational speed, data storage capacity and communication speed that have been achieved in the past fifty years. These risks are manifested in the use of cloud computing for data storage (as well as for other uses). The DTAG is mindful that data storage includes not only storage of information in databases but also the storage of data in devices attached to or making up the cloud. The location of cloud infrastructure in several different countries raises numerous legal questions relating to whether the storage of data in that infrastructure or the movement of data to, from or between devices attached to the infrastructure could involve unauthorized exports of technical data. Finally, the DTAG considered the benefits to industry and to Government of the use of cloud computing in terms of both cost and efficiency.

b. The DTAG reviewed several scenarios including the following:

- Company XYZ (located in the U.S.) engages with Cloud Computing Service Provider ABC (who may or may not have a presence in the U.S.) for its data storage needs (which include "technical data");
- Company ABC has cloud infrastructure located in the United States, Canada, United Kingdom, India and Brazil and communication links between the devices constituting infrastructure;
- The following questions arise from the scenario above:
  - What are the regulatory risks that XYZ will face in utilizing ABC for storage (and other uses) of technical data?
  - How can XYZ ensure its data is secure?
  - How can XYZ adapt to changing computing and storage needs?
  - What is the responsibility of ABC for protecting ITAR controlled technical data that is stored in the cloud?

2) Review the various cloud implementation arrangements

a. The DTAG reviewed the implementation arrangements and found that Cloud computing services are offered in multiple environments:

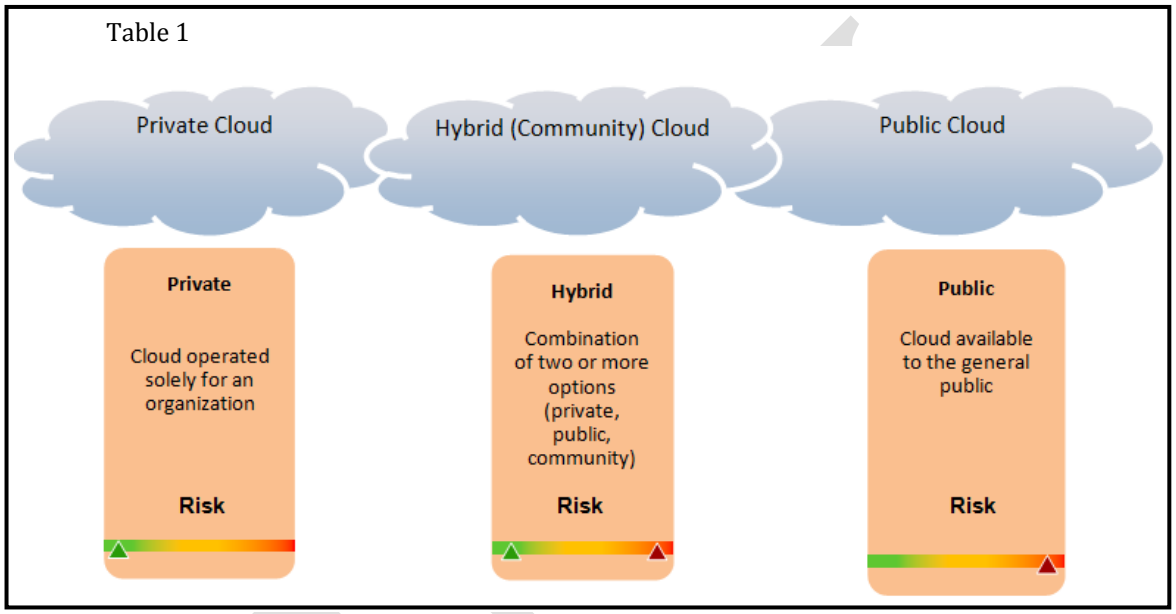
i. Public cloud – cloud infrastructure that is open to use by the public pursuant to standard terms and conditions that are applicable to all users. Public clouds also arise in two, more restrictive, forms.

1. Hybrid Cloud – This cloud is a combination of two or more cloud infrastructures that retain their own properties but enable data and applications to move across the multiple types of clouds.

2. Community Cloud – The Community Cloud infrastructure is intended for use by a specific community of consumers with shared interests, concerns or requirements.

ii. Private cloud – a cloud infrastructure that is open only to a specific class of users. Private clouds include cloud service providers that offer "ITAR compliant" services, which may include contractual obligations to locate all of the cloud infrastructure in the United States, utilize only network administrative personnel that are U.S. persons, encrypt data during transmission to, within and from the cloud, encrypt data at rest (wherever located in the cloud) and provide the contracting party with control of user authentication and access to data.

Table 1



b. The DTAG considered the benefits and potential risks associated with these environments including management and access control and determined that use of a Private cloud offers less risk than a Public cloud (including Hybrid and/or Community Cloud). This determination is based on the services and infrastructure being maintained on a private network with access limited to a specifically identified group. However, it is also the most expensive to implement in terms of software, infrastructure and maintenance. Additionally, many compliance risks inherent in electronic data storage reside in all types of cloud implementation arrangements. The DTAG outlined many of the questions that should be addressed by U.S. companies prior to engaging a Cloud Service Provider. (**See Attachment A**)

c. Using the aforementioned scenario, the DTAG evaluated the following::

i. Should XYZ Company engage with ABC, offering the Public, Private, Hybrid or Community cloud data centers?

1. Assuming that each cloud system has the same technical capabilities, the private cloud would allow XYZ the greatest control over the cloud however it would also be most expensive and least flexible to handle the needs of XYZ Company.

2. Alternatively, the DTAG evaluated the possibility that if the information is encrypted using a U.S. Government approved encryption method; this may provide the necessary security and access controls to allow storage of technical data in all of these environments.

3) Implications for Regulators

The ITAR was written at a time when the primary exchange of technical information was done in a physical way. Managing ITAR controlled technical data in a virtual world presents different risks that must be addressed to enable industry to utilize these tools in a compliant manner. Both Government and industry have existing and emerging cloud computing tools for design and development collaboration, information sharing, and project management that can be used to increase quality and efficiency. Regulators must address in the ITAR the practicality and necessity of doing business in a virtual world to enable industry and government to comply with the regulations while preserving as much as possible the benefits of cloud computing.

Consider the following with respect to use of the Cloud and Cloud Services:

- The Cloud is ubiquitous and is used in many aspects of our lives.
- The use of Cloud Services is pervasive in our daily business (to include the USG's daily business). Email, for example, is a cloud service.
- In today's business environment, there is almost no other way to share technical data without exposure to a Cloud unless we revert to USPS or any of the delivery or courier services.
- Because of the nature of the Cloud and how Cloud Services are provided, information transmitted into the Cloud can cross borders; information stored in the Cloud may be stored in other countries.
- Cloud Services are not transparent to the user, unless the user makes special arrangements with the Service Provider to have more visibility and control over how the information is handled; this can be expensive and may not meet all of the user's requirements (e.g., the ability to share technical data under license with a foreign person not in the U.S.).
- Without some recognized form of protection, companies may make inadvertent, unlicensed exports simply by placing technical data into the Cloud.
- The inadvertent, unlicensed exports are problematic for both the company and the regulator.

Besides the risk of inadvertent access, resulting in an unlicensed export when using Cloud Services, there are other security risks such as hacking into computer systems (personal, corporate, and in the Cloud) to get information, and insertion of malware to deny service, for example. However, these risks are well-recognized and have not deterred the use of Cloud Services. Prudent individuals and organizations take exceptional care to protect their systems and information from these risks. It seems logical that an update to the ITAR from a regulatory perspective to address cloud computing in a regulatory manner is in order.

One form of protection for technical data is encryption. The DTAG working group notes that the military uses strong encryption to protect classified data in electronic form. So, too, businesses can use encryption to likewise protect technical data in electronic form. For regulators, this means establishing the level of encryption deemed adequate for protection of technical data yet would still allow the use of Cloud Services. The ITAR currently does not address the use of encryption for the transmission or storage of ITAR controlled data via electronic modes. Standards for encryption exist today (e.g., FIPS 140-2), so regulators would only have to agree on the standard and the implementation. [Note: the working group recognizes there is a bit more complexity involved here, such as agreeing to the algorithm, the key length, the key management system, etc.]

Encrypting ITAR data at its point of origin secures it before ever transmitting it to the Cloud. Once in the Cloud, the encrypted data remains secure and protected unless or until access to the decryption tools are provided. Establishing a standard deemed acceptable to protect ITAR data while stored in the Cloud would protect it from unauthorized access and potential unintended export.

The following ideas were discussed within the DTAG:

a. Regulators could decide not to address the Cloud in the regulations and continue under the current regulatory conditions which implicitly either prohibit or restrict widespread use of the Cloud.

b. Regulators could set parameters for using Cloud Services and Cloud Service Providers for ITAR (and EAR) compliance.

c. Regulators could modify existing authorizations such as a license or exemption to specifically manage technical data within the Cloud.

d. Regulators could redefine the definition of "export" to exclude transmission or storage of encrypted ITAR controlled data.

e. Regulators could redefine "technical data" to recognize Cipher text (encrypted data) as being outside the scope of the current definition.

The DTAG determined that ideas a and c provided no enhancement or change to the existing methods being used today. With respect to regulators establishing parameters or standards for Cloud users and/or CSPs, the DTAG surmised that doing so would be outside the purview of the regulators. In addition, standards and parameters to identify key aspects of the arrangement such as roles and responsibilities and obligations upon contract termination should be identified within the Service Level Agreement (SLA) between the parties. GAO-210-513 and NIST Special Publication 800-144 provide recommendations on what the SLA should include.

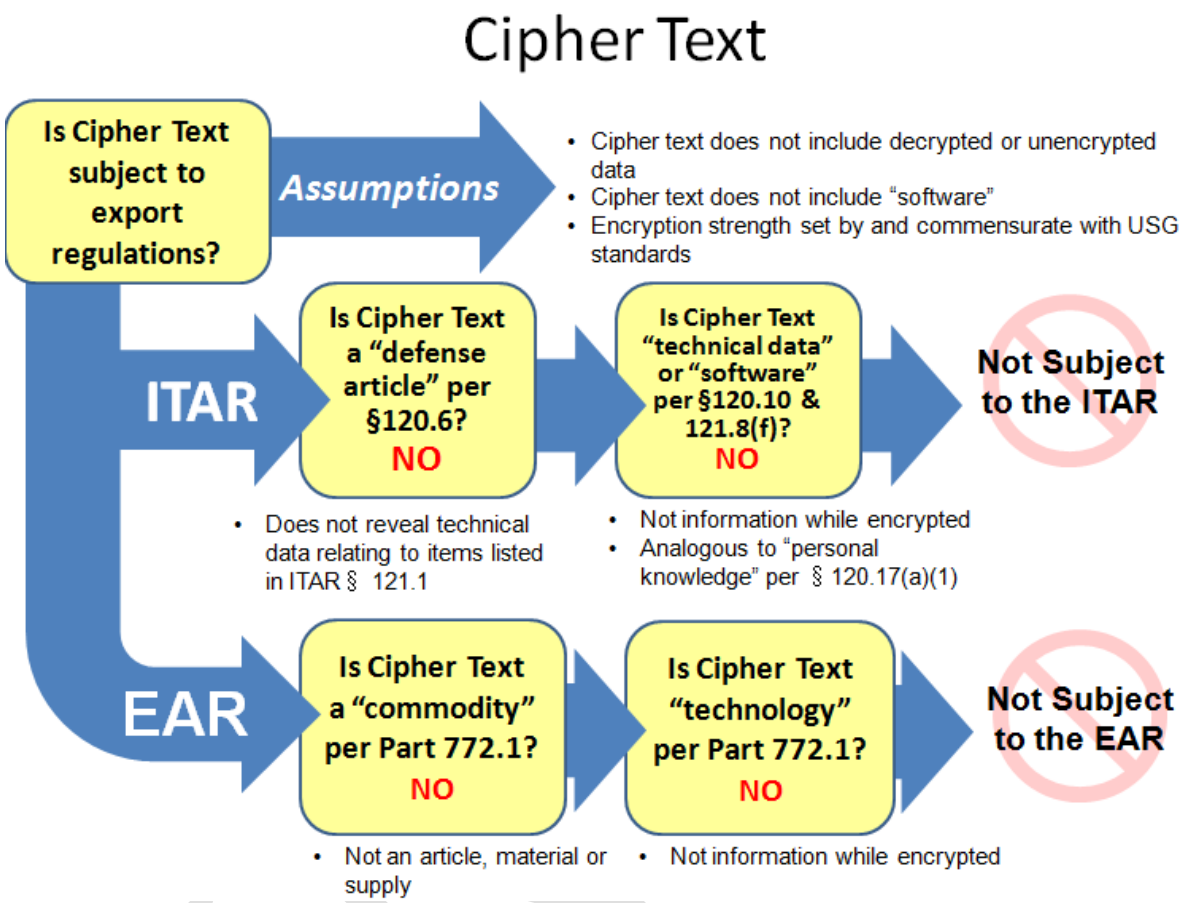
Having ruled out ideas a, b and c, the DTAG focused ideas d and e, considering encryption as the most viable method for addressing regulatory challenges related to ITAR controlled data being transmitted to and being stored in the Cloud.

It has been suggested that having the mere ability to 'access' ITAR controlled data presumes an export. Establishing a level of encryption deemed adequate to protect and secure ITAR controlled data would protect the Cloud user; enable full use of the Cloud for storage purposes; and protect the data from unauthorized access and the potential of an unintended export.

The user is placing their information in the Cloud, without knowing if, when, or where the CSP may 'move' their information to balance Cloud use. Encrypting ITAR controlled data to an established USG standard would protect the data from unintended access and unintended export in the event the CSP were to move it to a server outside of the United States. As a result, the DTAG believes that redefining 'export' to exclude unclassified, encrypted technical data being transmitted or stored outside of the United States provided that foreign persons are not provided with the access to the decryption tools is logical.

ITAR controlled data that is encrypted results in 'Cipher text', which contains a form of the original plain text, but is unreadable by human or computer without the tools to decrypt it. Based on Cipher text being unusable and unreadable by human or computer, the DTAG concluded that Cipher text does not meet the current ITAR definition of "technical data" nor is it within the scope of the AECA because it is unusable.

In addition, the DTAG went through the analyses of determining whether or not Cipher text is subject to export regulations using the following model and concluded that Cipher text is not subject to the export regulations.



As a result of our analyses, the DTAG proposes the following modifications to the ITAR:

§ 120.10 Technical Data

(b)(4) Unclassified, encrypted technical data being transmitted or stored, regardless of location, is not controlled under this provision provided that the data remains encrypted and the ability to decrypt the information is not disseminated. (See also § §120.17, 125.10)

§ 120.17 Export

Unclassified, encrypted technical data being transmitted or stored outside of the United States is not an export provided that foreign persons are not provided with access to the encryption tools.

§ 125.1 Exports subject to this part.

The controls of this part apply to the export of technical data and the export of classified defense articles. Information which is in the public domain (see § 120.11 of this subchapter and § 125.4(b)(13)), ***and unclassified, encrypted technical data, provided it remains encrypted during its transmission and storage, is not subject to the controls of this subchapter. If access to the encryption tool is provided to a recipient, a license or other authorization may be required.***

As a result of our discussions and review of various publications and information, the DTAG offers the following recommendation:

- The ITAR recognize encrypting data to an established standard as an adequate means of protecting and securing ITAR controlled data.
    - Unclassified, encrypted data transmitted or stored outside of the United States as not being an export, provided that foreign persons are not provided with access to the tools to decrypt it.
    - Unclassified, encrypted data is not subject to export regulations in this form.
    - Definitions for "export" and "technical data" are amended and that the transmission and storage of unclassified, encrypted technical data be reflected in ITAR 125.1(a).

The DTAG recognizes that there are other items needing further consideration to include:

- Alignment with other agencies to establish an encryption standard;
- Some companies or universities may not be able to meet encryption requirements and may need to use traditional methods to protect data;
- The mechanics of ensuring security still need addressed to include protection of tools and ensuring data stays encrypted in transit and at rest;
- Assessing potential impact if the USG were to change the encryption level standard; and
- Whether or not encrypted data in another medium would be an export if transferred/stored outside of the US.

4) Possible guidance that might be promulgated for use by exporters consistent with regulatory controls

- Cloud users should understand the different types of Clouds and service models and the export risks associated with each.
- Refer to NIST Special Publication 800-144 for recommendations on what the Service Level Agreement (SLA) with the cloud service provider should include.
- Roles and Responsibilities must be outlined and a means to audit the Cloud Service Provider should be established.
- SLA should identify Cloud Service Provider's obligations upon contract termination, such as the return and expunging of data.
- Cloud users should ensure the Cloud Service Provider can meet the Cloud user's requirements for managing ITAR controlled data.
- Cloud users should also ensure compliance with other US regulatory agencies.
- Cloud users should ensure that an adequate authentication process is implemented to protect access to company data and ITAR controlled data.

Summary

Through the DTAG's review on use of this data storage method and its various implementation arrangements it is clear that under today's regulatory framework, industry is seeking an update to the regulations to address compliance in a virtual business environment. The implications of cloud computing guided the DTAG to consider several possible regulatory responses that could offer increased security as well as stronger adherence to the intent of the regulations. Ultimately, the DTAG determined and recommended that establishing an encryption standard is the first step in addressing the regulatory challenges with using the Cloud as a means to store ITAR controlled data. Encrypting ITAR controlled data to an established level will then lead to the additional recommendations provided, along with consideration of the proposed modifications to the ITAR as noted above. Until the regulations are updated to reflect today's business environment, industry must work within the regulatory controls from a different era and apply those regulations as best as possible.

Publications, Articles and Case Law Reviewed, Discussed and Considered Pursuant to this Tasking

Center for Technology Innovation at Brookings, "Addressing Export Control in the Age of Cloud Computing", John Villasenor, July 25, 2011
Congressional Research Service, Cybersecurity Authoritative Reports and Resources, Rita Tehan, March 2013
DoD Cloud Computing Strategy, July 2012
GAO-10-513, "Federal Guidance Needed to Address Control Issues with Implementing Cloud Computing." May 2010
NIST Special Publication 800-38F, "Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping"
NIST Special Publication 800-53 "Recommended Security Controls for Federal Information Systems and Organizations", Rev. 3, August 2009.
NIST Special Publication 800-144 "Guidelines on Security and Privacy in Public Cloud Computing".
NIST Special Publication 800-145 "The NIST Definition of Cloud Computing".
NIST Special Publication 800-146 "DRAFT Cloud Computing Synopsis and Recommendations".
Nixon Peabody, "The Export Control Implications of Cloud Computing", Alexandra Lopez-Casero, August 2011.

Supplemental Materials Reviewed, Discussed and Considered

ITAR, 22 CRF 120
CNSS Instruction 4009, National Information Assurance Glossary
"ITAR and the Cloud", Candace Goforth presented at the SIA Fall 2012 Conference
"Emerging Technologies: Managing Export Controlled Data in the Cloud", C. Goforth, Bob Rarog, Matt Henson, November 9, 2012
"EAR Controls and Cloud Computing", Bob Rarog, Dept. of Commerce, BIS, SIA Fall 2012 Conference
Microsoft Office 365 "FISMA and ITAR Solutions for Enterprises," October 2012.

Attachment A

Questions Related to Export Risks in Cloud Computing Storage
Tangible Control
Where are the devices composing the cloud located?
Who controls physical access to the devices composing the cloud infrastructure?
What are the standards of access or controls on access to those devices?
Are the devices physically connected to other devices and if so, where are those devices located?
Intangible control
Who has administrative rights to each device composing the cloud? Where are they located and what are their nationalities?
What is the user access policy? Who controls the policy, who administers the policy? Where are those persons located and what are the nationalities of those persons?
What is the user authentication process? Who controls the process? Who administers the process and where are those persons located and what are the nationalities of those persons?
What are the standards for network security? Who sets those standards? Who administers those standards and where are those persons located and what are their nationalities?
Is data of one user physically or logically segregated from data of another user? Does that segregation apply to all devices composing the cloud and to electronic connections? Who controls this segregation, where are they located and what are their nationalities?
Can the user restrict or limit the locations where the user's data may be stored or can data be transferred to new locations without customer permission or knowledge?
Is data at rest encrypted? If so, to what standard?
Is data encrypted during transmission to, from or within the cloud? If so, what standard of encryption is used?
If encryption is used, who controls the encryption? Where are they located and what are their nationalities? Where in the use of the cloud does encryption/decryption take place?
Roles & Responsibilities
Is the user solely responsible for unauthorized exports of technical data resulting from storage etc., of technical data on the cloud?
Does the provider have responsibility for unauthorized exports of technical data resulting from storage etc., of technical data on the cloud?

Attachment B

Current Practice	Possible Future State (with Cipher text)
What is an export (in the context of cloud computing)?	
1. Sending or storing defense technical data out of the United States in any manner, except by mere travel outside of the United States by a person whose personal knowledge includes technical data; or 2. Disclosing (including oral or visual disclosure) or transferring technical data to a foreign person, whether in the United States or abroad; or	The DTAG agrees that an export takes place when the exporter provides the foreign person with technical data or provided encrypted technical data <u>with</u> a key to decrypt it. *Note: encrypted technical data, Cipher text, without a key, is not considered technical data, and therefore would not constitute an export of technical data if merely stored in the cloud.*
What is technical data?	
Per ITAR § 120.12 (1) Information, other than software as defined in § 120.10(a) (4), which is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles. This includes information in the form of blueprints, drawings, photographs, plans, instructions or documentation. (2) Classified information relating to defense articles and defense services; (3) Information covered by an invention secrecy order; (4) Software as defined in § 121.8(f) of this subchapter directly related to defense articles;	The DTAG recommends that the newly proposed definition of technical data be accepted to include the following provision: 1. Cipher text, also known as encrypted information, contains a form of the original plaintext that is unreadable by a human or computer without the proper cipher to decrypt it. 2. Cipher text <u>does not meet the definition of technical data</u> provided it remains encrypted. 3. In the event an authorized receiver decrypts the Cipher text it is controlled under the ITAR, as it becomes readable plaintext.
What is access to technical data?	
Under current industry practice, access to technical data may include inadvertent access or theoretical access such as that of an IT administrator.	1. The DTAG recommends that access is established only when the foreign person is able to access the data in plaintext or is provided with the cipher to decrypt the data. 2. The Cipher text transmitting on the cloud-computing servers is not technical data and therefore, no access can be gained.

Attachment C

Possible Strategies for Regulators

Options to Consider	Restrictions on Industry	Implementation "requirements" for USG	Perceived Risks	Benefits
No regulatory changes	Significant but implicit – ITAR does not provide guidance on Cloud or virtual storage/transmission	None	-Hacking of electronic data	None
Parameters for using Cloud Services and Cloud Service Providers	Significant & varied depending on extent of requirements	Significant & varied depending on extent of requirements	-Vary depending on parameters -Increased bureaucracy may not address actual risk	Seemingly greater "control"
Revised Definition of "Technical Data" to explicitly exclude Cipher text	None – Cipher text is not Technical Data and would not be subject to the ITAR	Standardize and publish minimum acceptable encryption level & key management infrastructure	Hacking of electronic data – no increase/decrease	Provides broadest use of cloud in a secure manner. Provides regulator with clear enforcement area.
Revised Definition of "Technical Data" definition to explicitly exclude Cipher text (with limitations)	126.1 countries	-- Standardize and publish minimum acceptable encryption level & key management infrastructure -- Users of Cloud and Service Providers need method to ensure no export to or import from 126.1 countries	- Hacking of electronic data – no increase/decrease - Different roles and capabilities of Cloud users and Service Providers to ensure no transmission to/from, access by, 126.1 countries - Confusing because contradictory to message about Cipher text	Although imposes some restrictions on Cloud usage, would allow freer usage & implementation
Revised Definitions of "Export" and "Import"	- None – if Cipher text is not Technical Data - Some if revised definitions have 126.1 limitations	- Standardize and publish minimum acceptable encryption level & key management infrastructure - If revised definitions have 126.1 limitations, then Users of Cloud and Service Providers need method to ensure no export to or import from 126.1 countries	-Hacking of electronic data – no increase/decrease -Different roles and capabilities of Cloud users and Service Providers to ensure no transmission to/from, access by, 126.1 countries	Provides broad use of cloud in a secure manner -If revised definitions have 126.1 limitations, then imposes some restrictions on Cloud usage, would allow some usage & implementation
License/license exemption	Various, possibly to include: 126.1 countries, possible recordkeeping	-Identify acceptable encryption for transmission of licensed data & key management infrastructure -Identify requirements for use of license exemption	Hacking of electronic data – no increase/decrease	Does not allow usage of most forms of cloud, except for private clouds with proper structure and controls.