NS2™
SAP NATIONAL SECURITY SERVICES
CLOUD

FAQ – SAP® PUBLIC

NS2 CLOUD® SUPPORT FOR ADHERENCE TO ITAR IN THE CLOUD

1. WHAT'S CONTROLLED UNDER THE ITAR AND THE EAR?

International Traffic in Arms Regulations (ITAR) control the export of defense-related articles (any item or technical data designated under the U.S. Munition List, as described in 22 CFR 121.1) and states that no non-U.S. person can have unlicensed access to technical data subject to ITAR. The Export Administration Regulations (EAR) place similar restrictions on the export of dual-use and commercial items designated on the Commerce Control List (15 CFR Part 772).

The ITAR's United States Munitions List (USML) includes equipment, components, materials, software, and technical information that can only be shared with non-U.S. persons under license authorization or, if available, a license exemption. The EAR's Commerce Control List (CCL) includes various commodities, software, and technology that may require a license (or license exception) to be exported or shared with non-U.S. persons.

The Department of State's Directorate of Defense Trade Controls administers and enforces the ITAR, while the Commerce Department's Bureau of Industry and Security implements and enforces the EAR.

In general, since it deals exclusively with defense-related items, the ITAR prescribes a more restrictive set of controls. Thus, cloud-based systems that serve both ITAR and EAR-controlled data must ensure that they meet the higher regulatory standards imposed by the ITAR.

A. HOW IS ITAR RELATED TO DATA?

The ITAR, of course, prohibits the unlicensed export of military weapons systems and other defense-related hardware. It also places similar restrictions on the transfer of technical data and information related to those military systems. While a fighter jet naturally falls under the ITAR, parts and subcomponents are also potentially export-controlled under the ITAR or the EAR. Design and manufacturing information may also be controlled under the ITAR as technical data.

ITAR technical data is defined at 22 CFR 120.10 as information which is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance, or modification of defense articles.

B. HOW DOES ITAR RELATE TO THE CLOUD?

Cloud computing services are not, as such, regulated under the ITAR. However, when such cloud computing services involve the storing and processing of ITAR-controlled technical data, the ITAR requires that such ITAR data not be inadvertently released or distributed to foreign persons or destinations outside the United States.

Any transfer of ITAR-controlled data outside of the United States (even if the data is simply processed through a server outside of the United States) is a violation of the ITAR's licensing requirements. Also, granting a non-U.S. person access to ITAR-controlled data within the United States is a violation of the ITAR (the so-called "deemed export" rule).

C. HOW ARE THE ITAR AND THE EAR ENFORCED AND WHAT ARE THE PENALTIES?

The Department of State Directorate of Defense Trade Controls (DDTC) oversees the enforcement of ITAR. The Department of Commerce enforces the EAR.

Violations of either the ITAR or the EAR can result in substantial civil or even criminal penalties. Violations may also result in debarment under the ITAR or a denial of export privileges under the EAR.

2. HOW DOES MY COMPANY KNOW IF IT HAS ITAR DATA?

It is the responsibility of the owner of the data to know what data is export-controlled technical data under either ITAR or EAR. Items that are controlled under the ITAR are enumerated or described on the USML (22 CFR Part 121), and any data that directly relates to any ITAR-controlled item is regulated as "technical data" under the ITAR. Determination of whether or not your company holds technical data for items on the USML is beyond the scope of this document. All manufacturers, exporters, and brokers of defense articles, related technical data and defense services on the USML must register with the DDTC. SAP NS2®, as a cloud provider providing data processing services, is NOT required to register with the DDTC.

3. HOW DOES THE NS2 CLOUD SUPPORT ITAR REGULATIONS?

The SAP NS2 Cloud® supports the ITAR regulations by providing an information system that is supported exclusively by U.S. persons. All SAP NS2 Cloud® computing hardware is located within the United States in data centers that have physical safeguards and controls in place to prevent physical access by non-U.S. persons.

SAP NS2® provides the logical access control mechanisms to your company in order to put in place logical access restrictions to prevent access by unauthorized personnel using commercially available off-the-shelf (COTS) technologies. While no technology is infallible, all reasonable effort is made to protect the SAP NS2 Cloud® from unauthorized access. The determination of whom and from where access is provided is largely based upon your company's requirements.

SAP NS2® works with its customers and can make recommendations based upon best practices such as having dedicated circuits using data-carrying technologies (i.e. MPLS) from a US telecommunications carrier, encrypting data traffic using FIPS 140-2 validated cryptographic module, and using a dedicated Virtual Private Network (VPN) tunnel with IPSEC encryption to protect data-in-transit between the SAP NS2 Cloud® and your company's data networks.

Potentially legitimate business requirements may require foreign access to a company's technical data; however, such ITAR technical data must be licensed for export to these specific foreign countries. Because of these situations, each ITAR customer presents varying challenges.

4. WHO OWNS ITAR RESPONSIBILITIES AND THE OVERALL SECURITY REQUIREMENTS?

Ultimately, responsibility for the security and protection of ITAR-controlled technical data falls on the owner of the information. SAP NS2® and its partners never become owners or brokers of the ITAR technical data. Your company should implement a Technology Control Plan (TCP) that prescribes how your ITAR-controlled technical data is to be protected. SAP NS2® has developed a TCP that describes how use of SAP NS2 Cloud® services protects ITAR technical data. Your company's existing TCP will incorporate the SAP NS2 Cloud® TCP.

5. WHO IS RESPONSIBLE FOR PROTECTING THE DATA?

SAP NS2® provides the technical mechanisms for protecting ITAR-controlled technical data, and we provide guidance on best practices to implement technical controls governing logical access to the cloud service. SAP NS2® implements all the physical and logical controls that protect the computing and data storage of the ITAR technical data. Your company must implement procedures that align with these technical mechanisms to restrict access only to authorized personnel according to these ITAR or EAR restrictions. Who can be granted access to this data depends entirely on: a) whether the data is ITAR or EAR-controlled; b) the destination country and the nationality of the person involved; and c) whether a license or license exception is available to authorize the data transfer.

6. WHAT HAPPENS IF MY COMPANY HAS OPERATIONS IN A FOREIGN COUNTRY (GLOBAL/DUAL COUNTRY/COMPANY)?

Absent a license from DDTC, the release of ITAR-controlled technical data is limited to U.S. persons as defined in 22 CFR 120.15. In lieu of a license, certain ITAR exemptions are available in limited circumstances. For example, an exemption at 22 CFR 125.4(b)(9) allows an employee of a U.S. company who is travelling abroad to access ITAR data on the company network provided that certain restrictions are fully met, including:

- **If the employee of the U.S. company is a foreign person, that employee must have been previously licensed to receive the data;**
- **The data must be transferred to the employee via secure network connections and appropriate safeguards, i.e., data encryption, must be used to protect the data;**
- **The employee must be directly employed by the U.S. company (not a foreign subsidiary), and the data can be used only by that employee and not shared with other persons; and**
- **The data cannot be used for foreign production or for the provision of a defense service.**

Transfer of ITAR-controlled technical data to a foreign person without a specific ITAR license authorization or an ITAR exemption constitutes a violation. Non-U.S. network administrators may not grant themselves access to ITAR-controlled data unless that data has been licensed for transfer to that foreign country and to the nationality of the network administrator.

Because a company's ERP system may store a broad range of technical data related not only to the company's products but also to particular customers' requirements, it can be challenging to craft an export license that includes the full scope of data held within an ERP system. Where a specific ITAR license or authorization is used to transfer data to a foreign destination, it is important to ensure that the scope of that authorization fully matches the range of data to be transferred.

7. WHAT IF MY PARENT COMPANY IS A FOREIGN COMPANY?

Foreign ownership of a U.S. company that manufactures ITAR-controlled items potentially present concerns for the U.S. government which may vary according to the level of sensitivity of those ITAR items. Agency concerns driven by foreign ownership of ITAR-registered companies are above and beyond the scope of this document.

As it relates to the IT management of systems and services that contain ITAR technical data, many companies have centralized their IT operations for efficiency or may use a "follow-the-sun" support model. This presents problems for IT systems that contain U.S. ITAR technical data. For example, a globally-managed enterprise Active Directory (AD) infrastructure that allows non-U.S. system administrators at the parent company to manage the AD's access control permissions violates ITAR authorization requirements because it allows domain administrators to grant themselves access to that ITAR technical data. While access log and auditing information may be used to provide alerts that such access had taken place, the ITAR technical data will already have been released and the violation will have occurred.

8. SHOULD MY COMPANY COMBINE OR SEPARATE ITAR FROM EAR-CONTROLLED DATA?

Many companies do store both ITAR and EAR-controlled technical data in their IT system, and that is permitted under the regulations. However, the ITAR currently imposes more stringent restrictions on access to controlled technical data by foreign persons, so any system that combines both ITAR and EAR data must meet the higher standards of the ITAR.

Hosting ITAR and EAR data on separate systems may be an alternative, but that approach has its own complications and limitations. There is a cost factor associated with having multiple IT systems, and the total cost of ownership or your company's support personnel should also be considered. Servers and support personnel need to be located within either the U.S. or an export-licensed country, and support personnel must be U.S. citizens or otherwise licensed to have access to the data on the system. It might be simpler and most cost-effective to have a one-way data feed from a non-ITAR-compliant system into an ITAR-compliant IT system. Data transferred out of the ITAR-compliant IT system would need to be scrubbed or otherwise sanitized of ITAR technical data. If data feeds leaving an ITAR-compliant IT system contain ITAR technical data, then those data feeds may result in the unauthorized release of controlled data to a non-U.S. person, which is a violation of the ITAR.

Overall, such judgements would need to be made by a subject matter expert in export compliance. SAP NS2® does not provide such subject matter experts but will work with your corporate export compliance personnel or outside experts hired by your company.

9. WHAT IS A "DEEMED EXPORT" AND WHAT ARE THE PENALTIES FOR VIOLATIONS INVOLVING DEEMED EXPORTS?

An export occurs whenever a controlled item or technology is transferred out of the United States. A "deemed export" occurs whenever controlled technology is released to a non-U.S. person within the United States. Under both the ITAR and the EAR, substantial civil fines or even criminal penalties can be imposed for violations involving either traditional exports or deemed exports. Violations can also result in debarment under the ITAR or a denial of export privileges under the EAR.

Export enforcement cases are listed on the websites of DDTC at the State Department and the Bureau of Industry and Security at the Commerce Department:

http://www.pmddtc.state.gov/compliance/poa.html

https://efoia.bis.doc.gov/index.php/electronic-foia/index-of-documents

A review of these enforcement cases reveals that a number of cases involve unauthorized transfers of export controlled technical data for foreign persons.

10. WHAT IS THE DIFFERENCE BETWEEN ITAR AND EAR?

The ITAR regulates the export of those military systems and selected parts or components that are specifically listed or described under one of the U.S. Munitions List's 21 categories; it also regulates the export of technical data and defense services related to those military items. The ITAR is administered by DDTC at the U.S. Department of State. In general, anything that is listed on the USML requires a license or an ITAR license exemption to be exported from the United States.

The Export Administration Regulations (EAR) regulate the export of commercial and selected "dual-use" items that are listed under any of one of the 10 categories in the Commerce Control Lists (CCL). The EAR is administered by the U.S. Department of Commerce. The CCL includes specific commodities, software, and technologies. License requirements under the EAR depend upon the specific classification of the item on the CCL and the destination to which it is to be exported. EAR license exceptions are often available in lieu of a specific license.

11. WHAT IS CUI AND HOW DOES IT RELATE TO NIST SP 800-171 AND THE CLAUSES IN DFARS 252?

NIST SP800-171, DFAR clause 252.204-7012, and DFAR clause 252.239-7010 all specifically deal with Controlled Unclassified Information (CUI). The CUI registry contains information regarding its categories, descriptions, and respective authority of controlled unclassified information and can be found here:

https://www.archives.gov/cui/registry/category-list

NIST SP 800-171 is the publication that focuses on protecting the confidentiality of Controlled Unclassified Information (CUI) in nonfederal systems and organizations, and identifies specific security requirements to achieve that objective. As of March 23, 2017, NIST Special Publication 800-171 Revision 1 is the latest publication of its security controls and can be found here:

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf

While NIST SP 800-171 applies to all federal government contractors holding contracts which invoke requirements to protect CUI, the DFAR clauses only apply to DoD contractors holding contracts which invoke the specific DFAR clause.

The DFAR clauses also uses the terms Covered Defense Information (CDI) and Controlled Technical Information (CTI). CTI is a specific category of CUI amongst the other categories and sub-categories of CUI. For DoD contract holders in which the DFAR clause is invoked, any cloud services utilized by the DoD contractor in performance of the contract is required to meet FedRAMP Moderate security control equivalents. This requires cloud providers to be meet the FedRAMP control required but not necessarily be FedRAMP-authorized.

Note as well that the Nuclear CUI category contains subcategories for unclassified Naval Nuclear Propulsion Information (NNPI), Unclassified Controlled Nuclear Information – Defense (DNCI), and Unclassified Controlled Nuclear Information – Energy (UCNI).

Furthermore, ITAR technical data and EAR technology are specific categories of CUI.

While CUI categories are mostly aimed at specifically protecting the government's information, the CUI category of Proprietary Business Information (PROPIN) aims to ensure the protection of data when a commercial company provides data to the government in order to prevent disclosure by the government under Freedom of Information Act (FOIA).

12. IF MY COMPANY PUTS AN APPLICATION INTO THE NS2 CLOUD, IS IT OK FOR ITS NON-U.S. BASED USERS TO ACCESS IT?

There is no single, simple answer to this question. Each scenario requires case-by-case review and, ultimately, compliance with the licensing requirements of the ITAR and the EAR is the responsibility of the user of any cloud-based service. SAP NS2 is not responsible for the customer's compliance with these export regulations.

As it relates to the ITAR, in most cases some form of ITAR authorization will be required to allow non-U.S. based users to access ITAR-controlled technical data in the cloud. ITAR license authorizations are specific as to the approved end-user and country. As noted in Q&A 6 above, in certain limited circumstances, an ITAR exemption may, for example, permit the employee of a U.S. company to access ITAR-controlled data stored in the cloud while that employee is travelling abroad. In the great majority of cases, however, some form of ITAR license authorization will be required to grant non-U.S. based persons access to ITAR technical data.

Where an ITAR license authorization or an ITAR exemption is not present, your company will need to implement appropriate technical mechanisms within the SAP NS2 Cloud® to prevent access to that specific ITAR technical data within the SAP NS2 Cloud® IT system. Such occurrences would need to be reviewed and handled on a case-by-case basis since the technical mechanism may be dependent upon the integration with the IT operations of the SAP NS2® customer.

NS2™
SAP NATIONAL SECURITY SERVICES

Email: info@sapns2.com
Phone: 877-972-7672

www.sapns2.com