

Addressing ITAR compliance with Teamcenter

Providing a framework for managing export control

www.siemens.com/teamcenter

white paper



- ▶ Teamcenter enables companies to securely manage sensitive information and other highly valued intellectual property in accordance with export regulations such as the U.S. International Traffic in Arms Regulations (ITAR). Regardless of whether suppliers, partners or company employees are working with your intellectual property, you can leverage Teamcenter to reduce the effort to comply with requirements for exporting regulated information – as well as with corporate policies for enforcing legal requirements documented in non-disclosure agreements and supplier contracts. Best practice companies approach security management as a strategic initiative that mitigates the legal and financial risks associated with sharing their intellectual property in support of their globalization objectives.

PLM Software

Answers for industry.

SIEMENS

Table of contents

Executive summary	1
Business challenges	2
Teamcenter's ITAR capability	3
Proven secure global virtual collaboration	6
Final evaluation	7
Standards-based glossary	8

▶ Executive summary

Today's business executives face a challenging dilemma. On one hand, they need to vigorously engage global partners in commercial initiatives to pursue many of industry's most promising revenue-generating opportunities. Typically, these opportunities involve forming strategic alliances with partners and suppliers to take advantage of both local and international competencies.

On the other hand, sharing information externally and exporting products require companies to comply with contractual obligations and regulatory requirements – such as the U.S. International Traffic in Arms Regulations (ITAR). When regulatory requirements are involved, companies and their decision makers face extremely high legal fines and even criminal penalties in instances of non-compliance.

Business executives need security management and export control solutions that mitigate the risks of regulatory non-compliance and provide the intellectual property (IP) rights protections required by their corporate governance and supplier contracts.

To address these issues, Teamcenter enables you to approach security management as a strategic business initiative that supports your globalization initiatives while mitigating their associated legal and financial risks. In pursuit of these objectives, Teamcenter delivers the following technology advantages and business benefits.

Teamcenter's export-related security advantages

Business value	Teamcenter advantage
Improves security	Enables administrators to restrict information access on the basis of terms and conditions specified by authorizing documents, including export licenses, technical assistance agreements (TAA), non-disclosure agreements and supplier contracts.
Reduces risk	Protects against future litigation by enabling enterprises to deliver proof of regulatory compliance (e.g. ITAR); also reduces potentially costly penalties by allowing enterprises to properly respond to legal discovery motions.
Increases productivity	Enables entitled users to easily and quickly find needed compliance data, while eliminating time wasted using outdated, inappropriate or irrelevant data
Reduces cost	Enables companies to lower administrative overhead associated ITAR compliance by providing a single point of administration and audit control

► Business challenges

Analyst estimates suggest that more than 35,000 regulations govern the auditing and retention of business information produced around the world. ITAR derives its authority from the Arms Export Control Act and Executive Order 11958. The U.S. State Department's Directorate of Defense Trade Controls (DDTC) administers ITAR and, under Section 121.1, establishes the United States Munitions List¹ (USML), which catalogues equipment, materials and technology (physical and information) that require DDTC approval for export. In addition, Section 126.1 establishes a list of countries to which no items on the USML can be exported. Some of the most important aspects of this regulation are:

Section 127.1(a) (1) of the Regulations provides that it is unlawful to export or attempt to export from the United States any defense article or technical data, or to furnish any defense service for which a license or written approval is required, without first obtaining the required license or written approval from the Office of Defense Trade Controls.

Section 127.1(b) of the Regulations provides that any person who is granted a license or other approval is responsible for the acts of employees, agents and all authorized persons to whom possession of the licensed defense article or technical data has been entrusted regarding the operation, use, possession, transportation and handling of such defense article or technical data abroad.

If your company works with foreign countries or employs foreign nationals, you need to understand ITAR and exercise due diligence to ensure that regulated information and items do not fall in the wrong hands. The first task is to understand what is covered by ITAR and to determine if your product, technology or service is on the USML. If so, then you need an export license or license exception to export the item anywhere in the world. Another aspect of this requirement relates to disclosing a USML item to a "foreign person" within the borders of the United States.

This activity is treated exactly the same as sending the item to the country where the foreign person has citizenship. In other words, under ITAR, an item can be "exported" even if it never leaves the United States. It is particularly important to understand this aspect of the regulation when foreign nationals visit your facility since you may unwittingly "export" your technology during the visit if you do not carefully limit visitor access to restricted information. You must also carefully manage foreign nationals in your employ to avoid unintentionally exporting a restricted item within your company.

Under ITAR, the definition of "export" comprehensively covers USML items falling in the hands of foreign nationals. This includes, but is not limited to, the sending or taking of a restricted material out of the U.S. in any manner and disclosing or transferring technical data to a foreign person, whether in the U.S. or abroad. In the case of information, "export" can be as benign as exposing data in a public forum (such as a webpage,) where it can be reviewed by foreign nationals. Also, any technical data covered under USML that is taken out of the country in any format (paper, laptop, removable drive) is treated as an export, even if it is never viewed by a foreign person. **See the DDTC's formal definition of "export" in this white paper's standards-based glossary for additional details or online at http://www.pmdrtc.state.gov/regulations_laws/itar_official.html.**

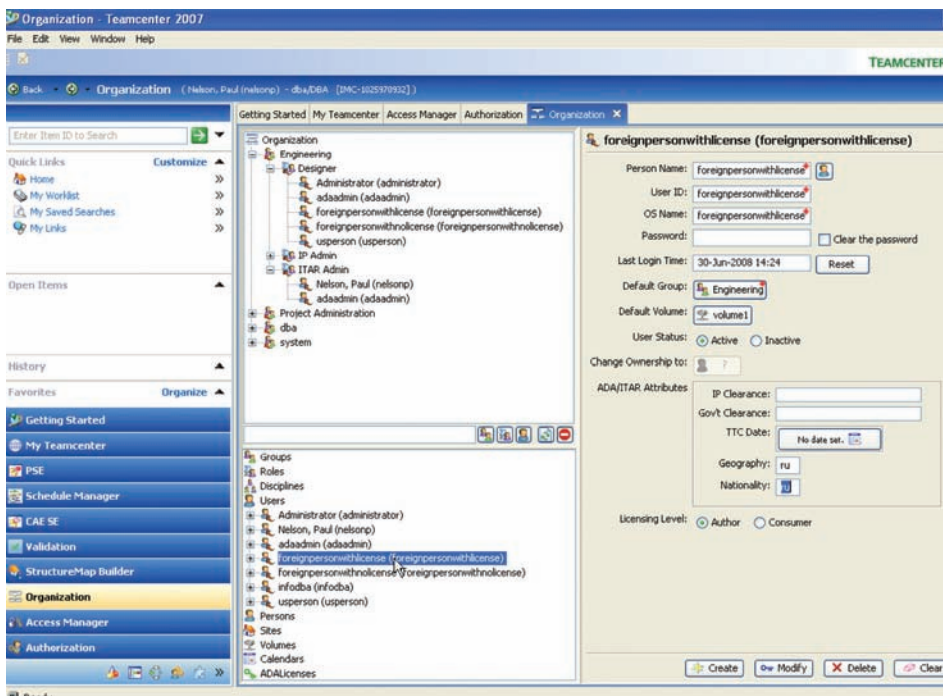
¹ Directorate of Defense Trade Controls, *International Traffic in Arms Regulations*. Official Version April 1, 2007 (http://www.pmdrtc.state.gov/regulations_laws/itar_official.html)

▶ Teamcenter's ITAR capability

Violating ITAR is considered a breach of national security and can result in criminal penalties under several different criminal statutes. In 2001, a major defense contractor was charged with 110 violations involving both ITAR and the Arms Export Control Act. The charges pertained to munitions and defense articles (i.e., technical data) exported to Australia, Singapore, Malaysia, Turkey, Spain and Italy. The contractor paid a civil penalty of \$4.2 million. In 1998, an Asian subsidiary of a major U.S. computer manufacturer pleaded guilty to violations of the International Emergency Economic Powers Act and the Export Administration Regulations relating to the unlawful export of computers to a Russian nuclear weapons laboratory. The company paid an \$8.5 million criminal fine.

Teamcenter provides a robust set of authentication, authorization and entitlement capabilities that you can use to define, control and secure access to sensitive data across your entire product lifecycle. Teamcenter's end-to-end lifecycle capabilities enable you to manage export control of sensitive material as an enterprise requirement from the earliest phase of your product development process through the delivery and support of the final product. Equally important, Teamcenter serves as the single source of all of your enterprise's product and process knowledge, enabling you to protect your enterprise's most valuable intellectual property by explicitly controlling who is allowed to access this information.

From a business perspective, Teamcenter enables you to rigorously and comprehensively enforce the rules and conditions articulated in authorizing documents, such as export control licenses, non-disclosure agreements and supplier contracts that underlie your company's globalization initiatives. Teamcenter's "Organization" application enables administrators to easily identify and control individuals or groups based on their national origin or physical location.



Using Teamcenter to easily classify people according to geography and nationality

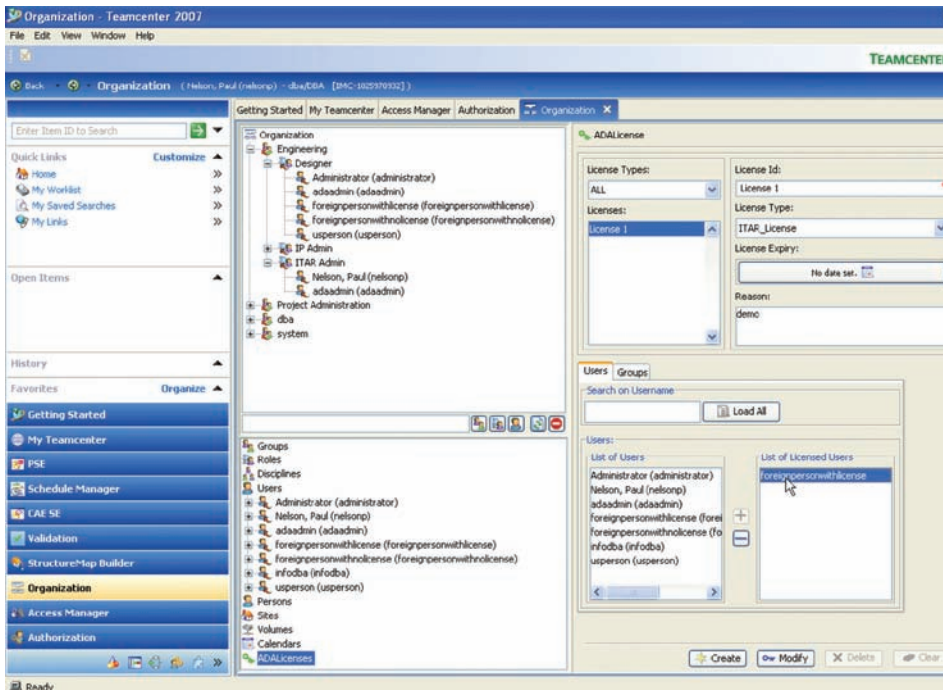
Teamcenter uses an Authorized Data Access model (ADA) to facilitate item access control via:

- Identification of users as restricted
- Identification of data as restricted
- Authorization of access to restricted data by restricted users using “authorizing documents” such as:
 - Export licenses
 - Technical Assistance Agreements (TAA)
 - Non-Disclosure Agreements
 - Contracts
- ADA access validation during any access attempt by restricted user

All information (including documents, CAD models and JT data) managed by Teamcenter can be controlled through ADA. Out-of-the-box rules restrict access of ITAR controlled items to “US persons.” A “foreign person” can be granted access to an ITAR controlled document through an authorizing document (export license).

Comprehensive and configurable auditing tools enable Teamcenter to log detailed user activities to an external log file or to the Teamcenter database, which can either be analyzed using Teamcenter’s reporting and analytics capabilities or processed by commercial off the shelf (COTS) tools.

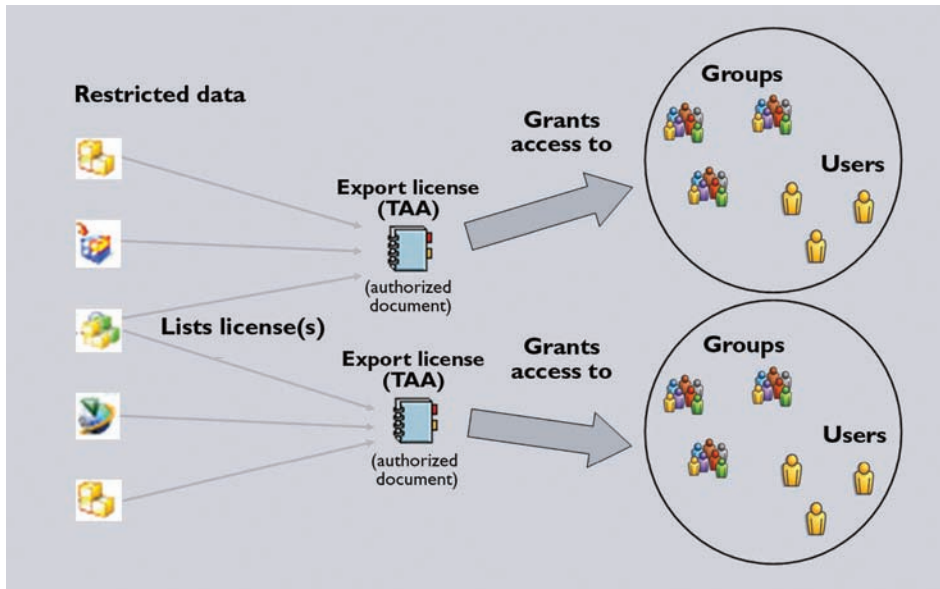
Using an export license, you can grant access of ITAR controlled items to an individual or a group of individuals.



Using the Organization application to enable an ITAR administrator to grant access to an ITAR-controlled document via a TAA

Within Teamcenter, an export license (TAA):

- Attaches legal content
- Acts as a gatekeeper for the release of restricted data
- Holds lists of authorized organizations and individual users
- Automatically revokes access upon expiration (thereby reducing administrative workload)



Teamcenter manages access to restricted information using “authorizing documents” such as TAA (export licenses)

The following Teamcenter capabilities establish a secure environment where your enterprise can share its intellectual capital with entitled suppliers and customers in accordance with ITAR and other legally binding restrictions.

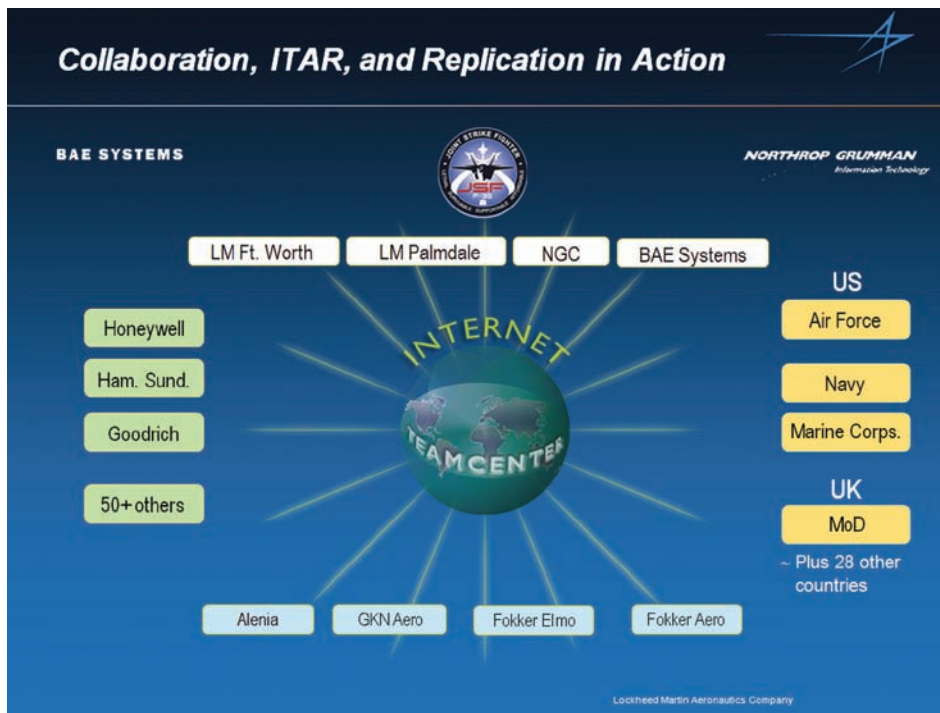
- **Authentication.** Teamcenter determines the identity of every user who attempts to access your PLM environment, making certain that every user is, in fact, who he or she is declared to be.
- **Authorization.** Teamcenter determines what information each user is allowed to access based on the user’s identity and/or the role, group, organization or project to which the user is assigned.
- **Authorizing document control.** Teamcenter can restrict information access on the basis of terms and conditions specified by given authorizing documents, including export licenses, technical assistance agreements (TAA), non-disclosure agreements and supplier controls. You can use Teamcenter to limit information access on the basis of the user’s nationality, geography and security clearance. You also can set expiration limits that restrict access in accordance with provisions in your authorizing documents.

Taken together, these Teamcenter capabilities provide the fine grain controls you need to protect your intellectual property, as well as the confidence you need to share information while vigorously pursuing a globalized business strategy.

► Proven secure global virtual collaboration

Led by Lockheed Martin, the F-35 program was designed to provide the U.S. Air Force, Navy and Marine Corps and the United Kingdom's Royal Navy and Royal Air Force with an affordable and stealthy tactical aircraft for the 21st century². Lockheed Martin partnered with U.S. and international aerospace leaders, including Northrop Grumman and BAE Systems, as well as almost 1,000 suppliers. In all, the parties involved in the production of the F-35 reside in more than 30 countries, spanning 17 time zones.

The first phase of the F-35 Collaboration Network deployment linked 5,000 users at facilities owned by the three primary partners and Stork Fokker of the Netherlands. These users are connected to the system with appropriate security safeguards to ensure compliance with ITAR requirements.



F-35 Collaboration Network for ITAR compliance

Teamcenter's rules help facilitate compliance with ITAR and proprietary control procedures. To date, more than 1,500 users across the extensive supplier network have been brought online, totaling more than 130 sites worldwide. Most importantly, real time online collaboration is a reality for both engineering in- process and released designs, across five major partners and 35 design suppliers. Lockheed Martin sees this as a critical program achievement.

² Extracted from *The JSF Digital Thread: A New Benchmark for Aerospace*, Tom Burbage, VP & GM, JSF Program, Lockheed, AvWeek Conference, Arlington, TX, October 2003.

► Final evaluation

As the foundation for the world's most widely used PLM portfolio, Teamcenter serves as the single source of all product and process knowledge. Teamcenter provides entitled users with instant access via a web browser to this knowledge at anytime from anywhere. ITAR functionality is an essential base feature of Teamcenter, allowing your enterprise to:

- Consolidate and control its product data
- Ensure that all users have appropriate security registration
- Manage the digital processes that distribute your product information
- Support a single security model

Equally important, Teamcenter:

- Helps you lower the administration costs associated with system security
- Facilitates compliance with applicable laws and regulations
- Supports industry standards and best practices

Teamcenter's ADA functionality is not limited to just export control; it enables companies to securely manage sensitive information (such as non-disclosure agreements and supplier contracts) and other highly valued intellectual property.

Access control lists (ACLs) – Identify authorized users and their respective privileges (granted, denied or not set)

Authentication – Process of determining whether someone or something is, in fact, who or what it is declared to be.

Authorization – Designates user access to various system resources based on the user's identity. Authorization is typically defined through the use of categories such as groups, roles and teams.

Authorized data access (ADA) – Authorized data access is an umbrella term that covers:

- Export control, e.g. ITAR
- Non-disclosure agreements
- Supplier contracts

Authorizing document –

- Attaches legal (e.g. licensed) content
- Holds list of authorized/restricted access groups and individual users
- Has expiration date
- Has activate/deactivate capability
- Facilitates automatic deactivation upon expiration

Entitlement – Designates user access to various system resources based on the user's identity. Authorization is typically defined through the use of categories such as groups, roles and teams.

Export³ –

- 1 Sending or taking a defense article 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 Transferring registration, control or ownership to a foreign person of any aircraft, vessel or satellite covered by the U.S. Munitions List, whether in the United States or abroad; or
- 3 Disclosing (including oral or visual disclosure) or transferring in the United States any defense article to an embassy, any agency or subdivision of a foreign government (e.g., diplomatic missions); or
- 4 Disclosing (including oral or visual disclosure) or transferring technical data to a foreign person, whether in the United States or abroad; or
- 5 Performing a defense service on behalf of or for the benefit of, a foreign person, whether in the United States or abroad.
- 6 A launch vehicle or payload shall not, by reason of the launching of such vehicle, be considered an export for purposes of this subchapter. However, for certain limited purposes (see § 126.1 of this subchapter), the controls of this subchapter may apply to any sale, transfer or proposal to sell or transfer defense articles or defense services.

³ Directorate of Defense Trade Controls, *International Traffic in Arms Regulations*. Official Version April 1, 2007 (http://www.pmdtc.state.gov/regulations_laws/itar_official.html)

Non-U.S. citizen (foreign person)⁴ – A person (as defined in § 120.14 of this part) who is a lawful permanent resident as defined by 8 U.S.C. 1101(a)(20) or who is a protected individual as defined by 8 U.S.C. 1324b(a)(3). It also means any corporation, business association, partnership, society, trust or any other entity, organization or group that is incorporated to do business in the United States. It also includes any governmental (federal, state or local) entity. It does not include any foreign person as defined in § 120.16 of this part.

U.S. person⁵ – A natural person who is a lawful permanent resident as defined in 8 U.S.C. 1101(a)(20) or who is a protected individual as defined by 8 U.S.C. 1324b(a)(3). It also means any corporation, business association, partnership, society, trust or any other entity, organization or group that is incorporated to do business in the U.S. It also includes any governmental (federal, state, local), entity.

Technical assistant agreement (TAA)⁶ – An agreement (contract) for the performance of a defense service(s) or disclosure of technical data, as opposed to an agreement of granting a right or license to manufacture defense articles. Assembly of defense articles is included under this section provided production rights or manufacturing know-how are not conveyed. Should such rights be transferred, § 120.21 is applicable. See part 124 of this subchapter.

⁴ *Ibid.*

⁵ *Ibid.*

⁶ *Ibid.*

About Siemens PLM Software

Siemens PLM Software, a business unit of the Siemens Industry Automation Division, is a leading global provider of product lifecycle management (PLM) software and services with 5.5 million licensed seats and 51,000 customers worldwide. Headquartered in Plano, Texas, Siemens PLM Software's open enterprise solutions enable a world where organizations and their partners collaborate through Global Innovation Networks to deliver world-class products and services. For more information on Siemens PLM Software products and services, visit www.siemens.com/plm.

Siemens PLM Software

Headquarters

Granite Park One
5800 Granite Parkway
Suite 600
Plano, TX 75024
USA
972 987 3000
Fax 972 987 3398

Americas

Granite Park One
5800 Granite Parkway
Suite 600
Plano, TX 75024
USA
800 498 5351
Fax 972 987 3398

Europe

Norwich House
Knoll Road
Camberley
Surrey GU15 3SY
United Kingdom
44 (0) 1276 702000
Fax 44 (0) 1276 705150

Asia-Pacific

Suites 6804-8, 68/F
Central Plaza
18 Harbour Road
WanChai
Hong Kong
852 2230 3333
Fax 852 2230 3210

www.siemens.com/plm

© 2008 Siemens Product Lifecycle Management Software Inc. All rights reserved. Siemens and the Siemens logo are registered trademarks of Siemens AG. Teamcenter, NX, Solid Edge, Tecnomatix, Parasolid, Femap, I-deas, Velocity Series and Geolus are trademarks or registered trademarks of Siemens Product Lifecycle Management Software Inc. or its subsidiaries in the United States and in other countries. All other logos, trademarks, registered trademarks or service marks used herein are the property of their respective holders.