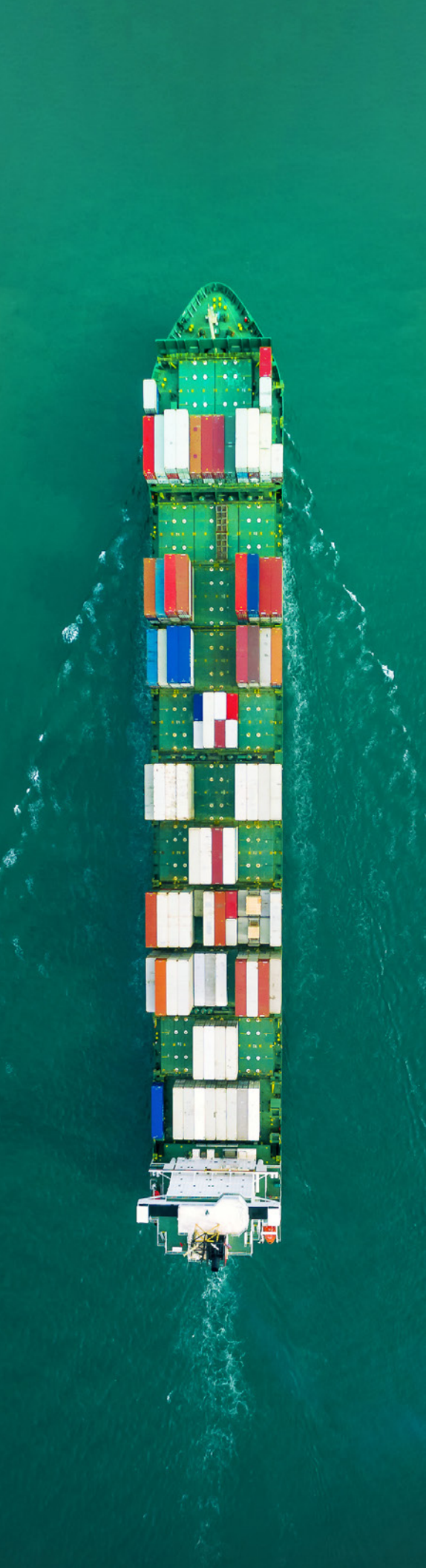
Hogan Lovells

Aerospace & Defense Insights

U.S. defense article and services trade regulator outlines expectations for global compliance

Beth Peters, Ajay Kuntamukkala, Anthony Capobianco, Aleksandar Dukic, Stephen Propst, Brian Curran, Julia Diaz, Josh Gelula, Deborah Wei



Through Aerospace & Defense Insights, we share with you the top legal and political issues affecting the aerospace and defense (A&D) industry. Our A&D industry team monitors the latest developments to help our clients stay in front of issues before they become problems, and seize opportunities in a timely manner.

The U.S. Department of State, Bureau of Political-Military Affairs, Directorate of Defense Trade Controls, which regulates the brokering, export, reexport, retransfer, and temporary import of defense articles and services, has published a manual detailing the essential elements of an effective risk-based compliance program. The guidance offers the A&D industry insights into the regulator's compliance expectations.

In December 2022, the U.S. Department of State, Bureau of Political-Military Affairs, Directorate of Defense Trade Controls (DDTC), the agency responsible for regulating the brokering, export, reexport, retransfer, and temporary import of defense articles and services, issued International Traffic in Arms Regulations (ITAR) Compliance Program Guidelines (the "Guidelines") which outlines eight elements DDTC considers to be essential for an effective risk-based compliance program.

Importance for A&D companies to build and maintain a compliance program

A robust ITAR Compliance Program (ICP) ensures that A&D companies and their staff who engage in ITAR-controlled activities do so in compliance with the ITAR, integrate ITAR requirements into their business and research process, and helps mitigate the risk of violating the regulations. Criminal and civil penalties for violating the ITAR are severe because such violations may harm U.S. national security and foreign policy objectives. Criminal convictions for willful ITAR violations can result in a maximum criminal penalty of US$1 million per violation, and/or imprisonment of up to 20 years. Civil penalties for ITAR violations can result in a fine of more than US$1.2 million per violation, and this amount increases annually to adjust for inflation.

Any ITAR violation, regardless of intent, may trigger administrative debarment actions. Debarment renders organizations and/or individuals ineligible to participate directly or indirectly in defense trade. Lastly, DDTC administrative settlements are posted publicly on DDTC's website, which may result in both negative publicity and reputational damage for the organizations.

Eight key elements of an ITAR compliance program

The DDTC Guidelines set forth the following ICP elements:

1. Management commitment;
2. DDTC registration, jurisdiction & classification, authorizations, and other ITAR activities; Other ITAR activities to be addressed in the ICP include:
   - Restricted party screening
   - Brokering
   - Reporting of political contributions, fees, and commissions
   - Cybersecurity and encryption for the protection of technical data
3. Recordkeeping requirements;
4. Detecting, reporting, and disclosing violations;
5. ITAR training;
6. Risk assessment;
7. Audits and compliance monitoring; and
8. ITAR compliance manual

Holistic compliance program approach

For decades, DDTC has provided guidance on ITAR compliance. DDTC priorities could be gleaned from an overview document called "Compliance Program Guidelines" and guidance and checklists generated in the DDTC acquisition notification process. DDTC has acknowledged that the eight elements in the Guidelines are focused on assisting organizations with ITAR compliance and recognizes that a company's activities may require compliance with multiple U.S. trade laws and regulations. These obligations are best served when the ICP functions effectively within the context of a holistic trade compliance program.

Specifically, in May 2019, the U.S. Treasury's Office of Foreign Assets Control (OFAC), the agency responsible for enforcing economic sanctions, published "A Framework for OFAC Compliance Commitments" (OFAC Framework) which outlines five components OFAC considers to be essential for an effective risk-based sanctions compliance program. The Hogan Lovells alert on the OFAC Framework is here. In February 2017, the U.S. Bureau of Industry and Security (BIS) updated the content of its Export Compliance Guidelines (BIS Guidelines). It provides details on the eight elements that BIS has determined are critical for an effective Export Compliance Program under the Export Administration Regulations (EAR). Each of these compliance frameworks and guidance documents have overlapping elements that can be layered into a comprehensive and robust trade compliance for companies in the A&D industry.

For example, the following elements have been addressed by each of DDTC, BIS, and OFAC in their compliance guidance:

- Management Commitment;
- Risk assessment;
- Recordkeeping;
- Training;
- Audits; and
- Handling violations and taking corrective actions

DDTC, BIS, and OFAC aim to ensure that company executives understand and promote corporate compliance through a top-down approach to U.S. trade control compliance. These guidelines are also consistent with those issued by the U.S. Department of Justice (DOJ). The Hogan Lovells alert on the DOJ policy is here. Additionally, on February 22, 2023 DOJ issued updated guidelines for United States Attorney's Offices regarding credit to be afforded companies when submitting voluntary self-disclosures here.

DDTC cybersecurity and encryption concerns

The ITAR does not explicitly require organizations to implement specific cyber security or encryption measures for the storage or transmission of technical data. However, certain exemptions may apply that necessitate encrypted data. The Guidelines contain a dedicated and separate section on cyber intrusion events, and explain that the theft of technical data may result in unauthorized exports. DDTC expects organizations to take steps to protect their technical

data from cyber intrusions and theft and consider carefully what cyber security solutions work most effectively for them. This section underscores the importance of this topic to DDTC and other agencies.

DDTC stressed that having specific policies, procedures, and tools for the encryption of technical data is a critical part of cyber security. Organizations should consider both how to encrypt the storage and transmission of technical data externally, and how to appropriately encrypt technical data on portable devices like mobile phones and laptops.

Importantly, Part 126 of ITAR requires organizations to promptly disclose the release of ITAR technical data to a number countries subject to arms embargo such as China. Where a breach is determined, or reasonably suspected, to involve one of these "proscribed" countries, mandatory disclosure requirements are implicated.

DDTC enforcement and practice tips

DDTC will consider the implementation of a risk-based tailored ICP program as a mitigating factor in an enforcement action. A robust ICP, both in terms of written policies and procedures and evidenced implementation, will be an important consideration for an A&D company in settlement or warning letter negotiations.

Whether in the context of an internal investigation or compliance more generally, A&D companies should encourage employees to report suspected ITAR violations. Further, A&D companies should regularly update their compliance programs to reflect regulatory changes, learning from published enforcement matters and business developments that trigger compliance reevaluation.

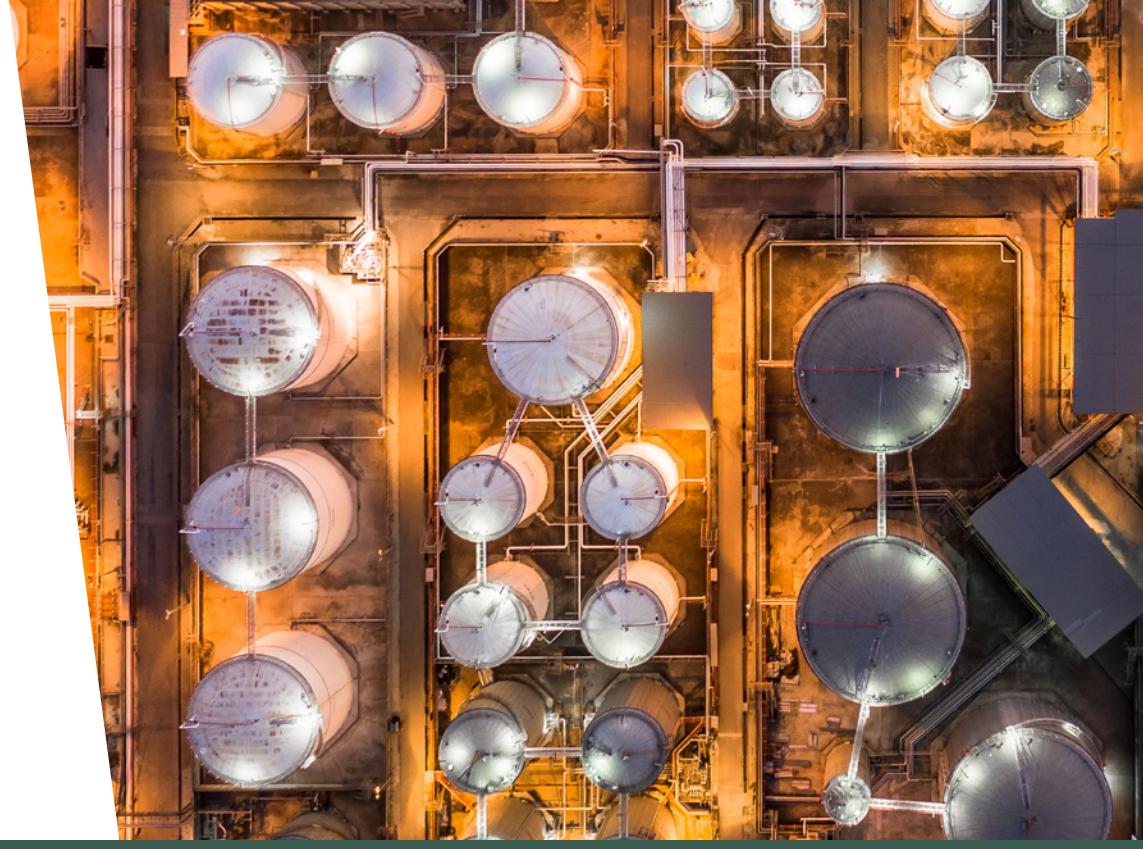
A robust ICP can be helpful in the voluntary disclosure process in demonstrating a commitment to compliance and in describing both the potential violation and how the ICP can be refined in response thereto. The disclosure should include mitigation efforts, such as retraining or reorganization of the responsible business unit(s), and describe any additional planned corrective actions that might address the root causes and prevent the recurrence of similar violations.

Conclusion

A&D companies should review the updated compliance guidance against their existing compliance program and procedures in considering the following:

- Assess, to the extent the Company is not already registered under the ITAR, whether registration is needed.
  - — Registration is required to use certain exemptions under the ITAR, including government contractor work. See Hogan Lovells article on the evolution of the ITAR exemptions for U.S. Government contracts.
  - — Registration is also required for domestic companies engaged solely in manufacturing ITAR items.
- Ensuring that their global ITAR compliance program is up-to-date and reflects the Guidelines and the eight elements.
  - — The Guidelines include helpful audit checklists organized by function.
- Establishing regular training for those responsible for ITAR compliance.
- Conducting risk assessments and gap analysis exercises to evaluate ITAR compliance, as well as EAR, OFAC and customs regulations compliance as applicable. (Companies should use the helpful audit checklists in the Guidelines which are organized by function.)

Because the DDTC Guidelines are similar to those issued by BIS and OFAC, A&D companies who may be new to the ITAR or who have only previously mapped their compliance programs against the guidance issued by BIS and OFAC, should review their policies and procedures to confirm that the elements set forth in the Guidelines are captured if they engage in ITAR regulated activities.



Beth Peters
Partner | Washington, D.C.
T: +1 202 637 5837
E: beth.peters@hoganlovells.com

Brian Curran
Partner | Washington, D.C.
T: +1 202 637 4886
E: brian.curran@hoganlovells.com

Ajay Kuntamukkala
Partner | Washington, D.C.
T: +1 202 637 5552
E: ajay.kuntamukkala@hoganlovells.com

Julia Diaz
Senior Associate | Washington, D.C.
T: +1 202 637 5499
E: julia.diaz@hoganlovells.com

Anthony Capobianco
Partner | Washington, D.C.
T: +1 202 637 2568
E: anthony.capobianco@hoganlovells.com

Josh Gelula
Counsel | Washington, D.C.
T: +1 202 637 6991
E: josh.gelula@hoganlovells.com

Aleksandar Dukic
Partner | Washington, D.C.
T: +1 202 637 5466
E: aleksandar.dukic@hoganlovells.com

Deborah Wei
Senior Associate | Washington, D.C.
T: +1 202 637 6468
E: deborah.wei@hoganlovells.com

Stephen Propst
Partner | Washington, D.C.
T: +1 202 637 5756
E: stephen.propst@hoganlovells.com

Alicante
Amsterdam
Baltimore
Beijing
Birmingham
Boston
Brussels
Budapest*
Colorado Springs
Denver
Dubai
Dublin
Dusseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Houston
Jakarta*
Johannesburg
London
Los Angeles
Louisville
Luxembourg
Madrid
Mexico City
Miami
Milan
Minneapolis
Monterrey
Munich
New York
Northern Virginia
Paris
Philadelphia
Riyadh*
Rome
San Francisco
São Paulo
Shanghai
Shanghai FTZ*
Silicon Valley
Singapore
Sydney
Tokyo
Ulaanbaatar*
Warsaw
Washington, D.C.

Associated offices*
Legal Services Center: Berlin

www.hoganlovells.com