U.S. Universities and the ITAR: Compliance Challenges and Best Practices

May 4, 2022

Jeff Trettin
Compliance & Civil Enforcement Division
Office of Defense Trade Controls Compliance

Application of the ITAR to Universities

- ITAR applies to all
  - Primarily regulates U.S. companies selling defense articles to non-U.S. militaries or governments
  - Applies to higher education and universities when their activities involve defense articles or services covered by the USML

- ITAR controls activities, such as:
  - Publishing research
  - Exchanging scientific information with researchers outside of the U.S.
  - Participation of a visiting scholar in a research project covered by the USML
  - Using equipment covered by the USML in laboratory
  - Research activities supporting foreign military or government (e.g., UAV payload)
  - Shipping equipment or material covered by the USML to a non-U.S. country

Balancing Open Research Culture and National Security Considerations

- Traditional university concepts:
  - Discover and expand knowledge for the benefit of humanity
  - Unrestricted academic freedom
  - Unrestricted academic publications
  - Unrestricted dissemination of research findings and results

- Universities conducting ITAR-controlled research must balance traditions of open access and dissemination of research with concerns about U.S. national security and foreign policy.

Reality on Campus: Types of Universities

University limits research conducted on campus

- Policy to conduct "fundamental research only"
- Declines research proposal or grant if it involves defense articles or services
- Declines proposals that require publication restrictions
- Will not undertake classified research
- Declines due to citizenship restrictions

University conducts ITAR-controlled research on campus

- Implements compliance program
- Appoints responsible senior administrators
- Trains professors and researchers
- Implements technology control plans
- Implements physical and IT access controls (e.g., lock door to laboratory)

Common Compliance Challenges for Universities

- Unaware of ITAR-controlled inventory or programs subject to the ITAR occurring on campus
- Human capital resources are experienced with limited bandwidth and many competing priorities
  - If one area of compliance requires attention, other compliance areas may be vulnerable
- Challenges investigating potential violations
  - Difficulty investigating activities on IT systems
  - Records are unorganized or difficult to access
- No or minimal audit capabilities
- Other dedicated compliance resources

Relationship between the State Department and Universities

- How does the U.S. Department of State support universities and their mission?
  - Investigate issues affecting universities
  - Direct outreach
  - Resources for universities
  - Mechanisms for universities to advise State

- How do universities contribute to State's enforcement objectives?
  - Mutually beneficial relationship
  - Universities voluntarily disclose suspected/actual violations of the ITAR
  - Universities voluntarily offer tips
  - Cooperation during investigations
  - Increased awareness and understanding of the regulations
  - Universities self identify weaknesses in their compliance programs so they can prevent and detect violations

State Department Resources Available to Universities

- DDTC's website - https://www.pmddtc.state.gov/ddtc_public
  - DDTC Response Team - ddtccustomerservice@state.gov
  - U.S. Department of State officials' participation in outreach events involving universities (Under Support tab of DDTC's website)
  - U.S. Department of State Company Visit Program campus visits (Under Support tab of DDTC's website)

Mechanisms for Universities to Advise the State Department

- Formal advisory group - Defense Trade Advisory Group (DTAG)
- Advisory Opinion requests
- Opportunity to comment on proposed regulations and new forms
- Opportunity to test new IT systems for export licenses and disclosures
- Ad hoc offer suggestions/ideas (e.g., redesign website)

Consequences of Non-Compliance

- Potential harm to U.S. national security & foreign policy
- Potential adverse impact on institutional reputation and the ability to obtain future federal research funds
- Potential civil enforcement actions resulting in fines and penalties

ITAR Compliance Program Elements

ITAR compliance programs should address:

1. Organizational structure
2. Compliance resources
3. Product classification
4. Contracts/marketing screening
5. License preparation & implementation
6. Exemption Implementation
7. Non-U.S. person employment
8. Physical security of the ITAR facility
9. Computer network security
10. Foreign travel
11. Foreign visitors
12. Foreign students
13. Record keeping
14. Reporting
15. License / Agreement maintenance
16. Shipping & receiving processes
17. ITAR training
18. Internal monitoring and audits
19. Voluntary Disclosure
20. Violations and penalties
21. Brokering

Key Factors of Effective Compliance Programs

- Senior management commitment to compliance
- Established policies and procedures
- Experienced personnel and training to maintain knowledge base
- Adequate resources dedicated to compliance

Key Factor – Senior Management Commitment

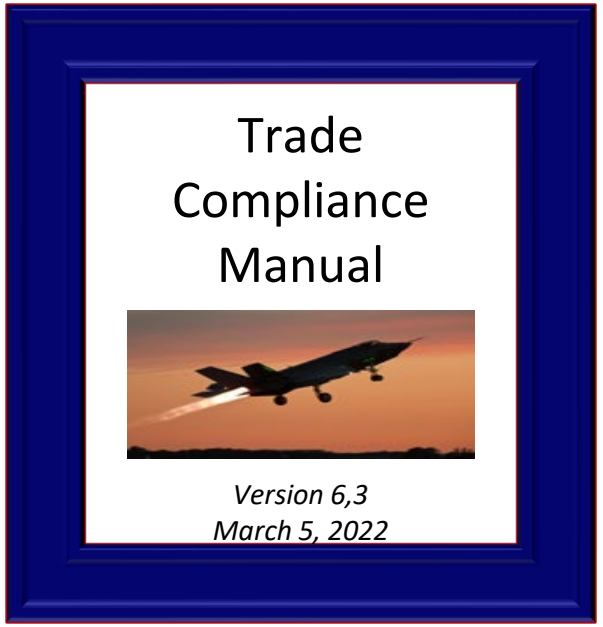
Senior management is responsible for creating culture of compliance

- Have general knowledge of export controls
- Directly engage in ITAR registration and disclosure responsibilities, as appropriate
- Dedicate adequate resources to compliance program & activities
- Create an organizational structure that incorporates compliance as a significant function
- Consistently message importance of compliance
- Encourage employee reporting without retaliation
- Reward compliance successes with incentives

Senior Management Commitment (Continued)

- Human Resources
  - Responsible & knowledgeable personnel
  - Job Descriptions
  - Annual Evaluations
- Material Resources
  - Budget
  - Training
  - Dedicated Positions
- Messaging
  - Senior Management Statement of Commitment
  - Senior Management/Board Reporting and Involvement
  - Training

Key Factor - Policies & Procedures



The best compliance programs are tailored to the organization.

They don't need to be complicated – they need to work.

Key Factor - Policies & Procedures

Policies & Procedures Should Be:

- Tailored to the business or university
- Designed for each functional area at every site
- Accessible, easy to understand, effective, and not overly burdensome
- Written, tested, and regularly improved
- Dynamic, not static

Written Procedures

- Written procedures, available to all personnel involved in activities, addressing such areas as:
  - Senior Management Statement
  - Jurisdiction/Classification
  - License Determination
  - Technical Data/Technology Control
  - Training, Monitoring & Reporting

Key Factor – Experienced Personnel & Training

- One size does not fit all
- Tiered, documented training program
  - Awareness training for all/most
  - In-depth training for subject matter experts
  - Focal points for additional information
- Frequency: regularly scheduled and as needed
- Ensure trainers are subject matter experts

Key Factor - Experienced Personnel & Training

Training Implements the P&P

Comprehensive Training Plan:

- Function specific
- Awareness for all
- Advanced training
- Outside training
- Online modules

Goal of Training:

- Maintain & improve knowledge base
- Compliant employees
- Prevention of Violations

Key Factor - Training

Training Issues to Consider:

- Train technical experts for the classification process
- Train the trainers
- Recordkeeping – presentation and attendance
- If do not attend training, what happens?
- Test attendees' subject matter comprehension
- Adequate resources to effectively train
- Do NOT overlook training for university leadership

Train to Protect Your Electronic Technical Data

- **Risk areas:**
- Employee onboarding
- Employee departure or role change
- Foreign employees, students, visitors, or third-parties with network access
- IT consultants
- Travel with electronic devices

Prevention:

- Technology Control Plans (TCP)
- IT Automation tools
- Maintain records of screening and users with access to tech data
- Log tech data access
- Obtain authorization for anticipated access
- Remove tech data from devices when unnecessary

Key Factor – Adequate Resources

- Staffing – the right number of people, in the right roles, with the right experience and training
- Infrastructure and security:
  - Information Technology – systems are secure and allow technical data to be handled and stored correctly
  - Physical security – the site is secure and defense articles and technical data are handled and stored correctly
- Budget covers regular costs of compliance

Defense Trade Advisory Group (DTAG)

- In May 2020, DTAG published a white paper containing recommendations regarding DDTC's Compliance Program Guidelines (CPG).
- In October 2020, DTAG published a white paper containing a draft compliance Risk Matrix.
- Both white papers are available on DDTC's website under the "Lean about DTAG" tab.
- DTCC appreciates DTAG's efforts, and it is currently drafting updated CPG and a Risk Matrix that draw on DTAG's recommendations that it intends to publish this year.

Contact Information

- For all other matters, including substantive questions and inquiries regarding registration submittal or status and referrals, contact the **DDTC Response Team**
  - Phone number: (202) 663-1282
  - E-mail: DDTCCustomerService@state.gov

- For general information, please visit DDTC's website
  - http://www.pmddtc.state.gov/