2026 Summer Back to Basics

Trade Compliance Programs

Jennifer K. Weinel
Northrop Grumman Corporation

Conference Agenda

We are here in the transaction process!

- Trade Compliance Programs →
- Submission Tools →
- ITAR Registration (as required) →
- Jurisdiction and Classification →
- ITAR Exemptions/ EAR Exceptions →
- ITAR/EAR Licensing →
- ITAR Agreements →
- Customs Clearance →
- Disclosures and Enforcement

Distribution Limited to SIA Members/Attendees and Subject to SIA Code of Conduct

Why Have a Trade Compliance Program?

Reasons to have a Trade Compliance Program

- Helps reduce the chances of trade violations
  - Protects U.S. national security & promotes U.S. foreign policy objectives

- Mitigating factor in any enforcement actions if a violation occurs

- Competitive business advantage

Potential Export Penalties

Fines	Criminal	Civil
State/ITAR	• Up to $1M per violation • Up to 20 yrs imprisonment	• § 127.10(a)(1)(i) - $1,271,078 (or 2x value of the transaction, whichever is greater) • § 127.10(a)(1)(ii) - $1,055,721 (or 5x payment, whichever is greater) • § 127.10(a)(1)(iii) - $1,256,607 • Extra compliance measures
Commerce/ EAR	• Up to $1M per violation • Up to 20 yrs imprisonment	• 50 USC 1705(b) – IEEPA – Up to $377,700 per violation (or 2x value of the transaction, whichever is greater) • 50 USC 4819 – ECRA – Up to $374,474 per violation (or 2x value of the transaction, whichever is greater)

- Loss of export privileges
- Debarment and/or suspension
- Reputational harm – loss of revenue & jobs

Distribution Limited to SIA Members/Attendees and Subject to SIA Code of Conduct

Tailoring your Program to your Organization's Needs and Risks

- Factors that will impact your Trade Compliance Program:

Items, End-use, & End-user

Volume of Exports

Geographic locations of org., sub, and customers

Relationships with business partners

Size of Organization

Complexity of Export Processes

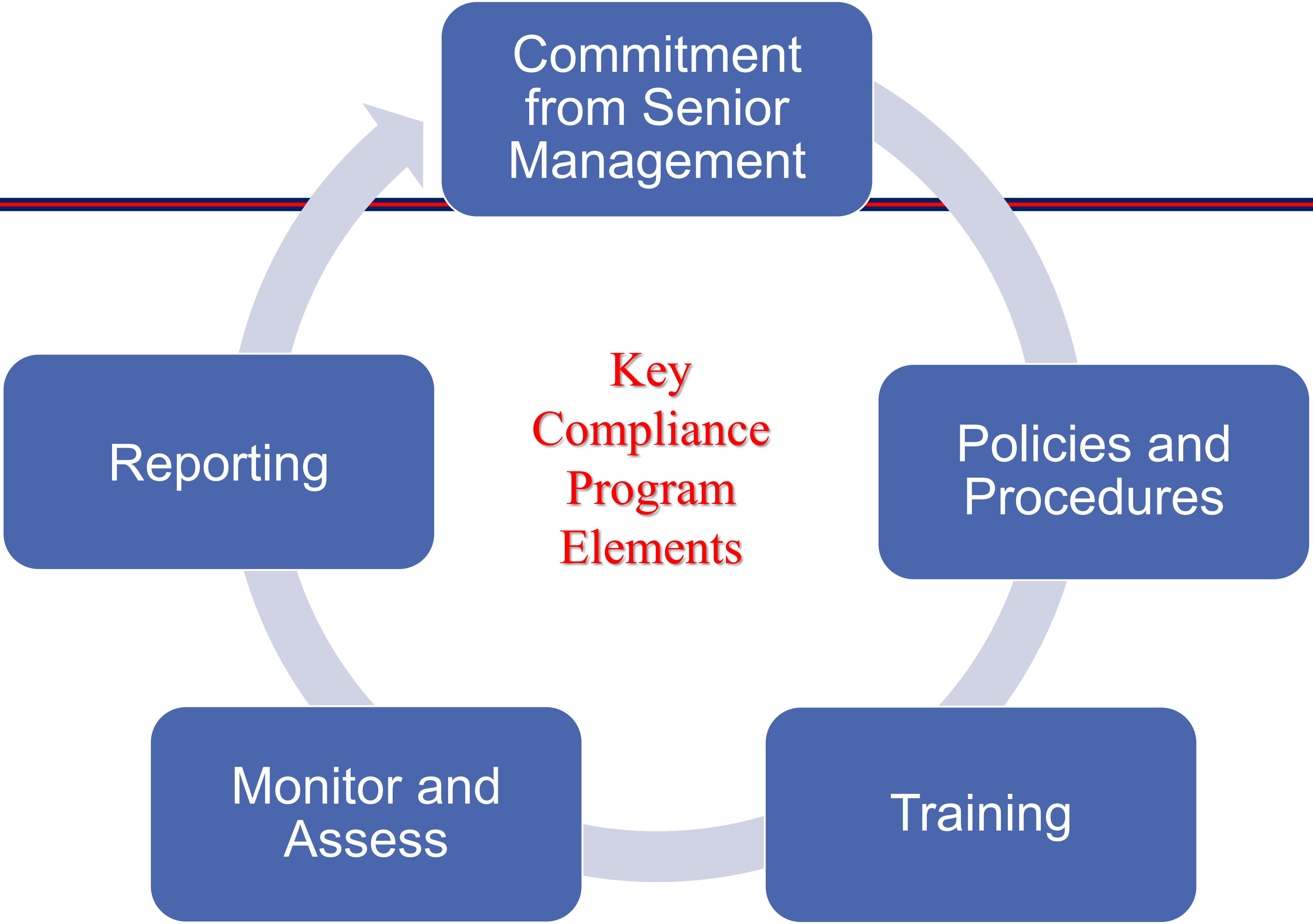
KEY ELEMENTS OF A TRADE COMPLIANCE PROGRAM

Distribution Limited to SIA Members/Attendees and Subject to SIA Code of Conduct

Elements of an Effective Compliance Program

- **Element 1:** Management Commitment
- **Element 2:** Jurisdiction & Classification, Licensing/Authorizations (Registration/Other ITAR)
- **Element 3:** Recordkeeping
- **Element 4:** Reporting and Addressing Violations
- **Element 5:** Training
- **Element 6:** Risk Assessment
- **Element 7:** Audits and Compliance Monitoring
- **Element 8**: Export Compliance Manual and Templates (Procedures)

More information available on DDTC's website - DDTC Compliance Program Guidelines and BIS's website - BIS Export Compliance Guidelines


Commitment from Senior Management
Policies and Procedures
Training
Monitor and Assess
Reporting
Key Compliance Program Elements

MANAGEMENT COMMITMENT

Management is responsible for creating culture of compliance

- Have general knowledge of export controls
- Dedicate adequate resources to compliance program & activities
  - Experienced people, budget and training.
- Create an organizational structure that incorporates compliance as a significant function
  - Include compliance in Job Descriptions and Annual Evaluations
- Provide consistent message of the importance of compliance and encourage employee reporting without retaliation
- Acknowledge compliance successes

Policies & Procedures

Policies & Procedures Should Be…

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

Distribution Limited to SIA Members/Attendees and Subject to SIA Code of Conduct

Written Procedures

- Elements should track to Compliance Program Guidelines
  - Management Commitment, Jurisdiction & Classification, Licensing/Authorizations, Recordkeeping, Report Violations, Risk Assessment, Audits/Monitoring
  - Due Diligence and Denied Party Screening
- In addition, partner with and embed export requirements in other functional procedures
  - R&D/Engineering for Jurisdiction & Classification
  - Bus Dev and HR for licensing
  - IT for data/technology controls

DATA/TECHNOLOGY CONTROLS

Protect your electronic technical data from unauthorized release

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

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

Due Diligence and Screening

- Screening is good, but not enough – vet/know your parties
  - Use checklists and questionnaires
  - See EAR 732, Suppl. 3 - Know Your Customer Guidance and Red Flag Indicators
  - Educate staff on “Red Flags” or suspicious transactions and how to escalate to resolve
- Screen all Parties to the Transaction (including freight forwarders, intermediate consignees, and the ultimate consignee)
  - Consolidated Screening List Tool
  - Maintain screening record results
  - Have a process to resolve “false positive” hits
  - Vendor software screening programs may be preferable for larger volumes
  - Vet/screen early and often (Automate rescreens, if possible)
- Don't Let this Happen to You!, BIS Settlements and ITAR Consents
  - Enforcement | Bureau of Industry and Security

Due Diligence and Screening (Consolidated Screening List)

Commerce – BIS

- Denied Persons List
- Unverified List
- Entity List
- Military End User (MEU) List

State

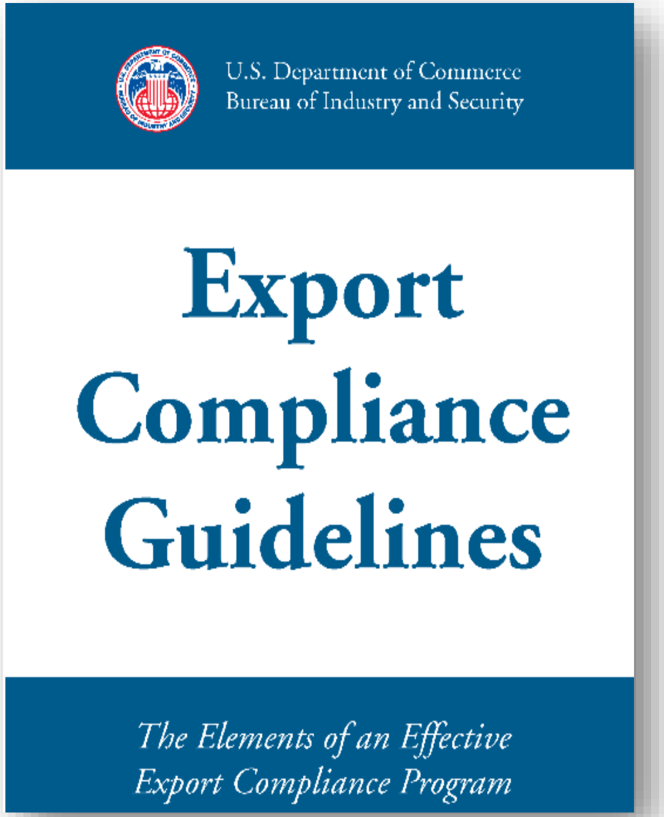
- Nonproliferation Sanctions
- AECA Debarred List

Treasury - Office of Foreign Assets Control

- Specially Designated Nationals List
- Foreign Sanctions Evaders List
- Sectoral Sanctions Identifications (SSI) List
- Correspondent Account or Payable-Through Account Sanctions (CAPTA) List
- Non-SDN Menu-Based Sanctions List (NS-MBS List)
- Non-SDN Chinese Military-Industrial Complex Companies (CMIC)
- Palestinian Legislative Council List

BIS Export Compliance Program Review

- BIS EMCD staff will review your manual
- Provide strengths and suggestions
- 30 days to receive feedback
- Mitigating factor for administrative penalties
- Send to EMCD@bis.doc.gov



More information available on BIS' website. Link to Guidelines: BIS Export Compliance Guidelines

TRAINING

Goal of Training is:

- Maintain up-to-date knowledge base
- Ensure observant and capable employees
- Identification and prevention of violations

Comprehensive Training Plan:

- General awareness for all
- Function/role specific for some
- Advanced training for key personnel
- Outside training if needed
- Online modules may be helpful

Risk Assessments

- Risk Assessments
  - Past incidents and disclosures
  - Changes in regulations
  - Areas of USG enforcement emphasis
  - New business opportunities, new countries involved, product offerings, etc.
  - Prioritize risks identified - Consider likelihood and consequence should a risk be realized
  - Develop plan to mitigate risks

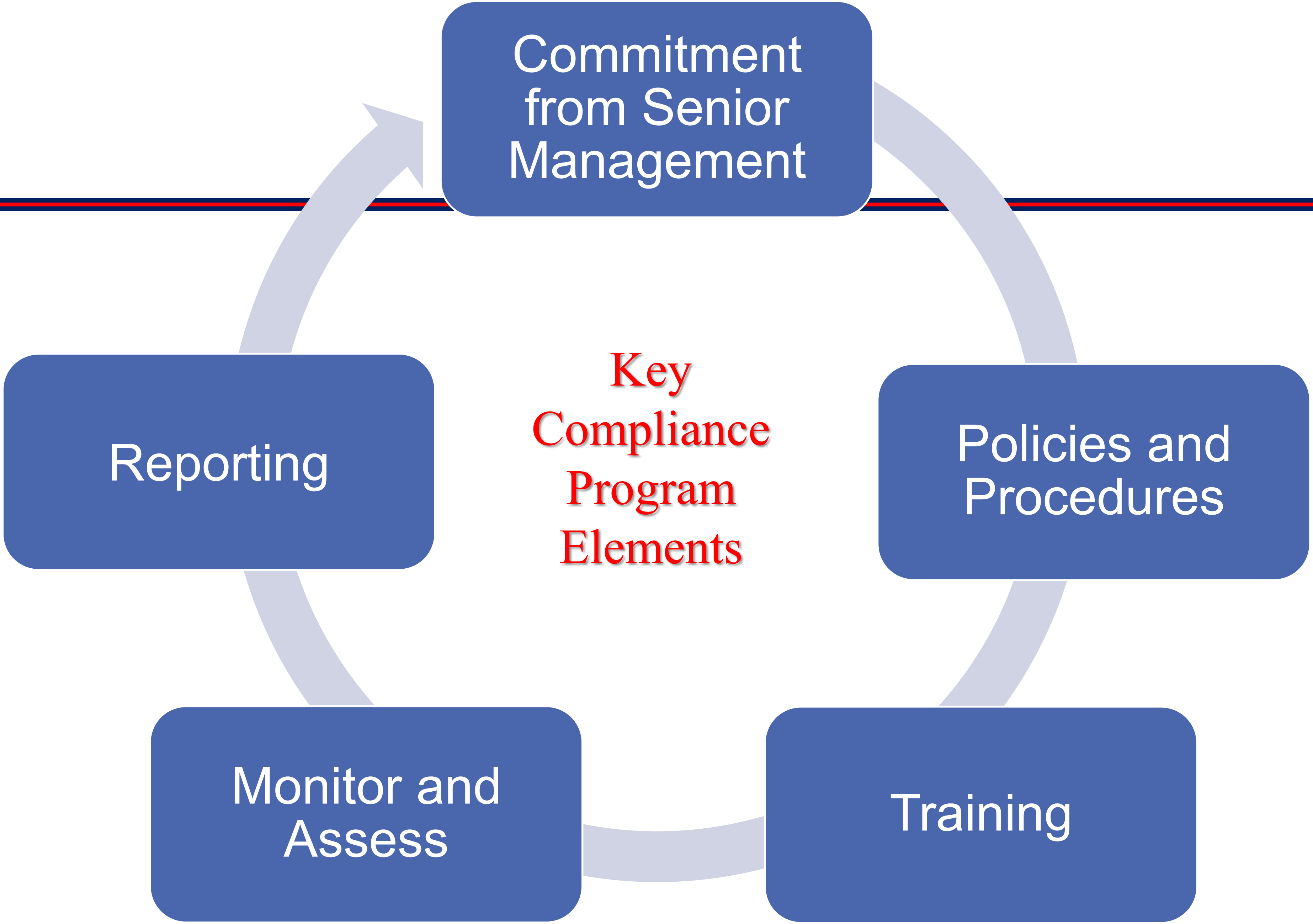
AUDITS AND MONITORING

- Audits and Monitoring
  - Regularly assess (procedures, licenses, programs, product lines)
  - Assess functions that support International Trade
  - Document findings, track corrective actions to completion
  - Use as a training tool and share lessons learned

REPORTING

Establish:

- System(s) to identify and report suspected violations
  - Include anonymous reporting mechanism
  - Automated tools help identify violations and decrease human error
- Process for investigating (and disclosing) violations
- Process to track implementation of corrective actions with accountability


Commitment from Senior Management
Policies and Procedures
Training
Monitor and Assess
Reporting
Key Compliance Program Elements

Q&A