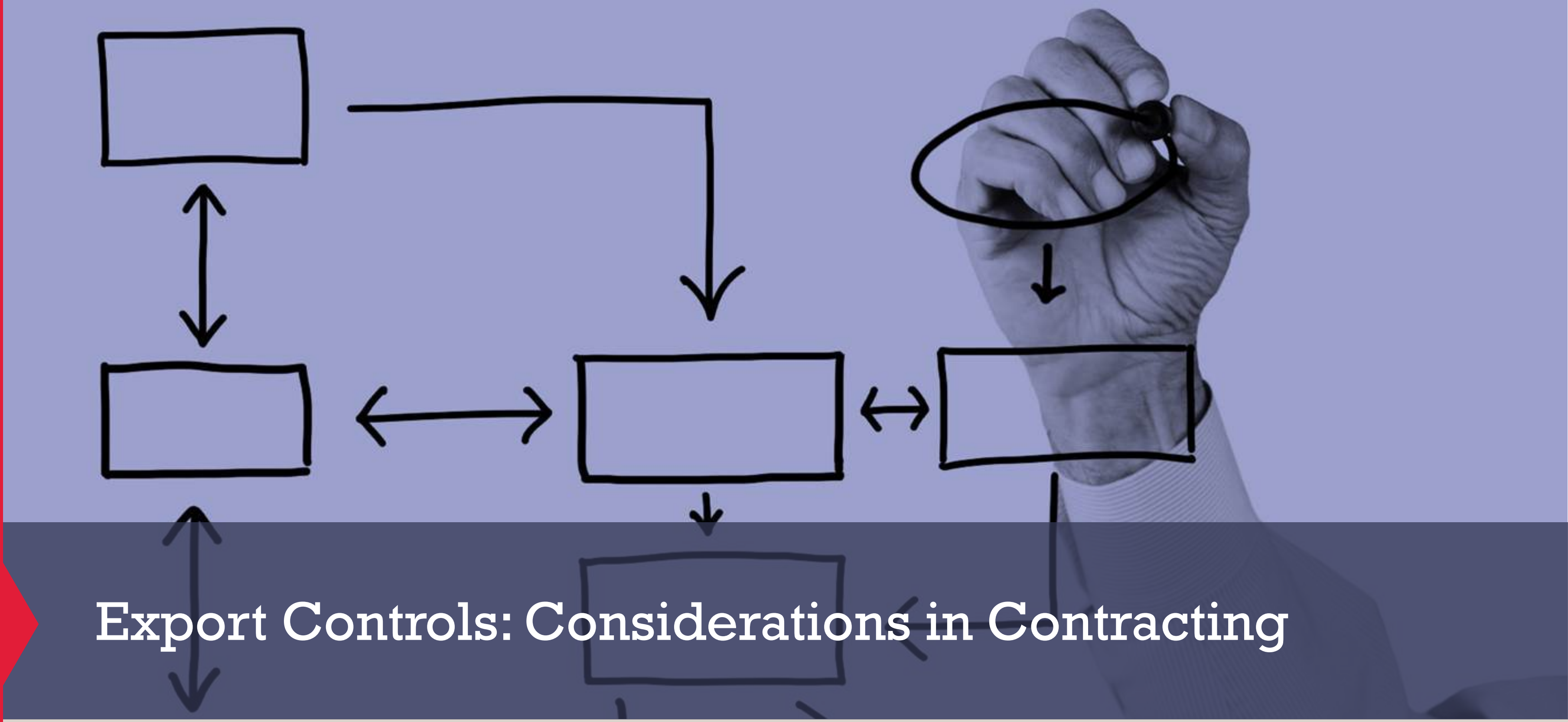


# Export Controls: Considerations in Contracting

**Susan Wyatt Sedwick, PhD, CRA, CSM**
Consulting Associate
Higher Education and Academic Medical Centers
Attain, LLC

NSPAA Conference

June 9, 2016

ATTAIN
Proven Performance. Forward Thinking.

# Overview of Export Controls Regulations & Sanctions

# What laws are we addressing?

International Traffic in Arms Regulations (ITAR)

Department of Defense Trade Controls

Export Administration Regulations (EAR)

Sanctions and Embargoes (OFAC)

# Risks for Universities

- Collaborations/discussions with foreign national collaborators and students especially when involving proprietary information
- Taking or shipping items or transferring technology that is controlled to a foreign country or foreign national
- Performing defense services
- Visiting scientists
- Travel to foreign countries including fieldwork and instruction
- Technology and material transfers
- Faculty "start up" companies

# Deemed Exports

- "Deemed Export" – foreign national with access to information restricted by EAR/ITAR.
  - Applies to a research assistants and students
  - Applies to visiting foreign researchers
  - Applies to U.S. citizens visiting a foreign country
- Does not apply to U.S. Citizens, permanent residents and those with US asylum protection

# What is controlled?

## ITAR

- Items on the Munitions List
- Includes both research on *defense articles* and training or assistance in developing *defense articles*
- Technical data related to the manufacture or production of *defense articles*
- Anything with a substantial military application or related to satellites

## EAR

- Dual Use Technologies
- Scope of the EAR

# Exclusions and Exceptions

## Exclusions

- Information in the Public Domain
- Fundamental research
- Educational Exclusion
  - Catalog courses and instructional labs
- Foreign patent applications

## Exceptions

- EAR
  - Temporary (TMP) *Tools of the Trade*
- ITAR
  - If ordered under federal contract §126.4 (c)

# NSDD 189

## National Security Defense Directive 189

‘Fundamental research' means basic and applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community, as distinguished from proprietary research and

from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons

# *Bona fide* Employee Exemption (ITAR)

- Applies only to the transfer of technology but not the associated "defense service" making it virtually useless
- Full time regular employees of US institutions of higher education with permanent abodes in US throughout employment
  - Must be informed in writing and agree not to transfer technology to another foreign national without a license
  - Does not apply to foreign graduate students
  - Does not apply to foreign nationals from prohibited countries

# Travel Abroad

- Equipment
  - Laptops, handhelds, and encryption products
    - Most publicly available software is not subject to export controls under the EAR (Source code v. Executable code)
    - https://wikis.utexas.edu/display/ISO/International+Travel+Guidelines
  - Data/technology
  - Blueprints, drawings, schematics
- Controlled technologies/data at a "closed" conference or meeting (not open to all technically qualified members of the public where attendees are not permitted to take notes and registration fees are “reasonable”)
  - Conferences in Iran and Cuba
- Money transactions and the exchange of goods and services in certain countries
- Travel to sanctioned/embargoed countries
- Denied persons and entities

# Securing Laptops and Handhelds

## BEFORE

- Use a loaner or purchase a new hard drive/phone
- Check for Encryption Restrictions
- Update security patches and backup
- Leave sensitive information at home

## DURING

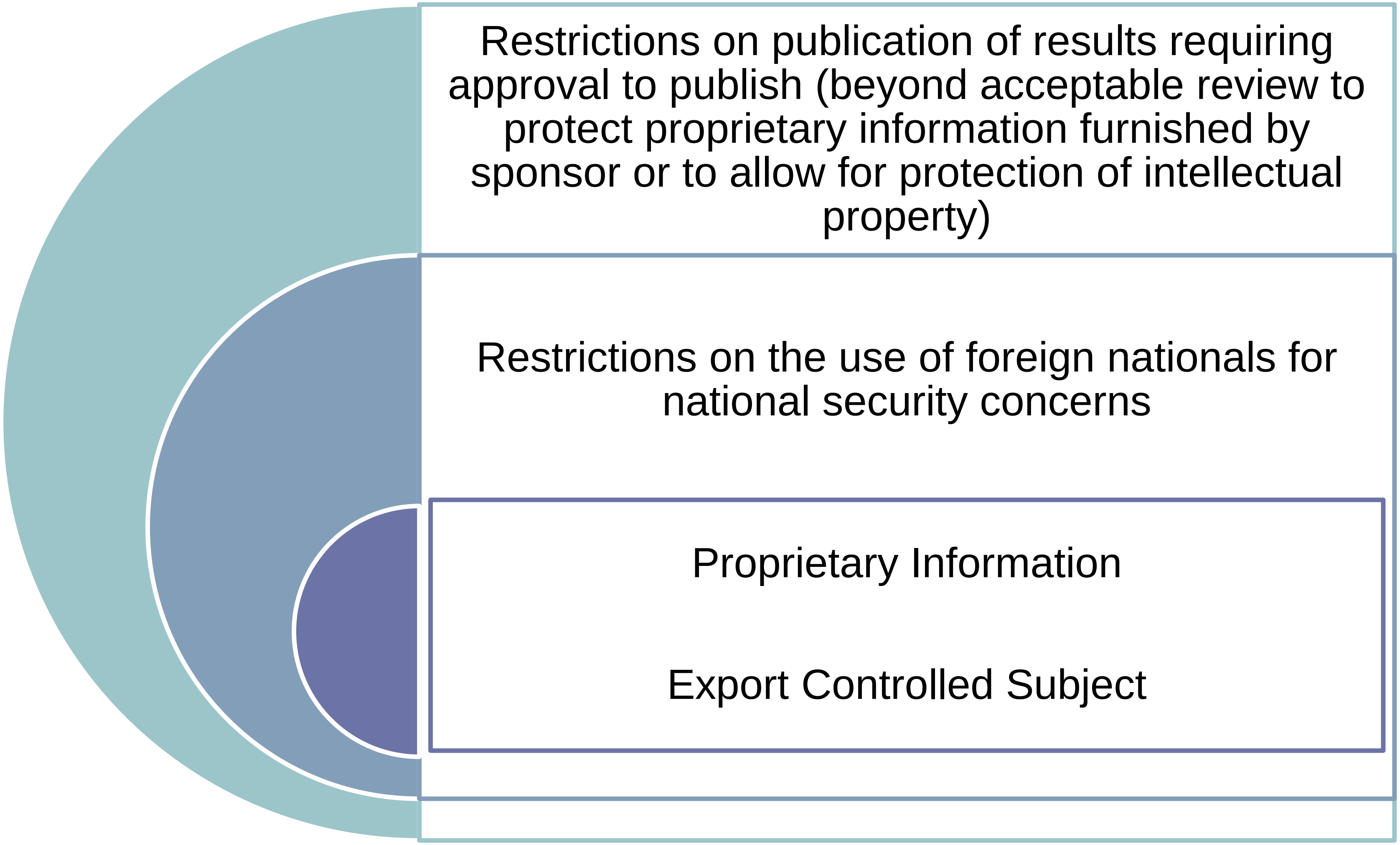
- Check networks carefully before connecting
- Keep list of credentials used
- Avoid portable storage
- Control access

## AFTER

- Assume your computer has been compromised
- Clean hard drive and erase all credentials
- Report suspicious activity

# Contracting Pitfalls

# Troublesome Clauses



Restrictions on publication of results requiring approval to publish (beyond acceptable review to protect proprietary information furnished by sponsor or to allow for protection of intellectual property)

Restrictions on the use of foreign nationals for national security concerns

Proprietary Information

Export Controlled Subject

# DFARS 252.204-7000 Disclosure of Information (August 2013)

( a) The Contractor shall not release to anyone outside the Contractor's organization any unclassified information, regardless of medium (e.g., film, tape, document), pertaining to any part of this contract or any program related to this contract, unless—

(1) The Contracting Officer has given prior written approval;

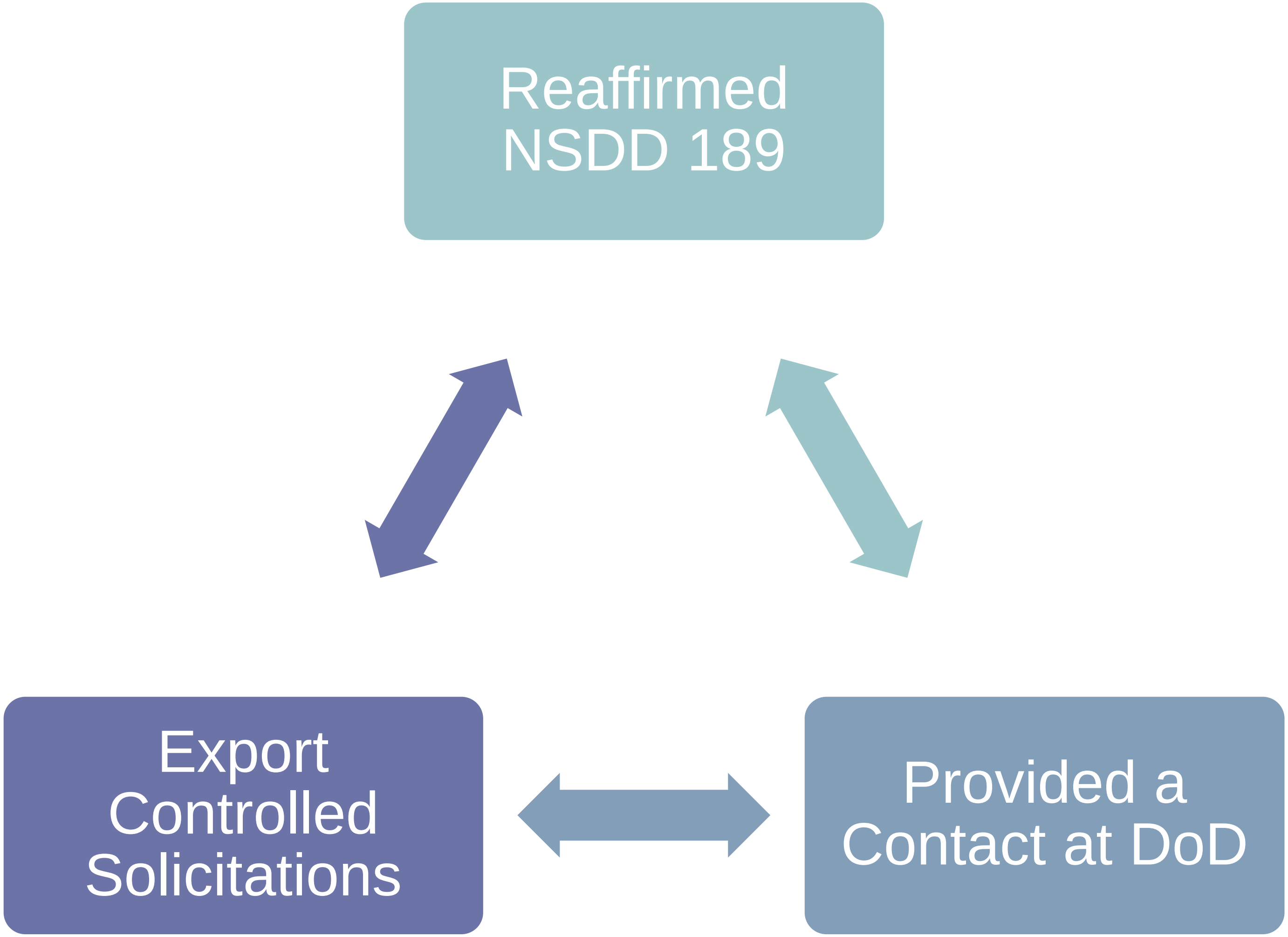
(2) The information is otherwise in the public domain before the date of release; or

(3) **The information results from or arises during the performance of a project that has been scoped and negotiated by the contracting activity with the contractor and research performer and determined in writing by the contracting officer to be fundamental research in accordance with National Security Decision Directive 189, National Policy on the Transfer of Scientific, Technical and Engineering Information, in effect on the date of contract award and the USD (AT&L) memoranda on Fundamental Research, dated May 24, 2010, and on Contracted Fundamental Research, dated June 26, 2008.**

(b) Requests for approval under paragraph (a)(1) shall identify the specific information to be released, the medium to be used, and the purpose for the release. The Contractor shall submit its request to the Contracting Officer at least 10 business days before the proposed date for release.

(c) The Contractor agrees to include a similar requirement, including this paragraph (c), in each subcontract under this contract. Subcontractors shall submit requests for authorization to release through the prime contractor to the Contracting Officer.

# Ashton Carter Memo



Reaffirmed NSDD 189

Export Controlled Solicitations

Provided a Contact at DoD

# NARA Proposed Rule on Controlled Unclassified Information (CUI) - RIN 3095-AB80

- Confidential Unclassified Information was originally defined by Executive Order 13556 published in 75 FR 68675 on November 4, 2010 with implementation by agencies
- National Archives and Records Administration (NARA) proposed rule published May 8, 2015
- Requires reporting of non-compliance
- CUI Registry

*Planned single FAR clause to flow down requirements to federal contractors*

# DFARS 252.204-7012

## Safeguarding Covered Defense Information and Cyber Incident Reporting

- Prescriptive requirements
- References security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, “Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations
- *Cyber incident reporting requirement requires* “rapid reporting” within 72 hours of discovery of any cyber incident.
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, “Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations
  - Deadline for Compliance: December 31, 2017

# NARA Definitions

### Controlled Unclassified Information (CUI)

- Information that laws, regulations, or Government-wide policies require to have safeguarding or dissemination controls, excluding classified information

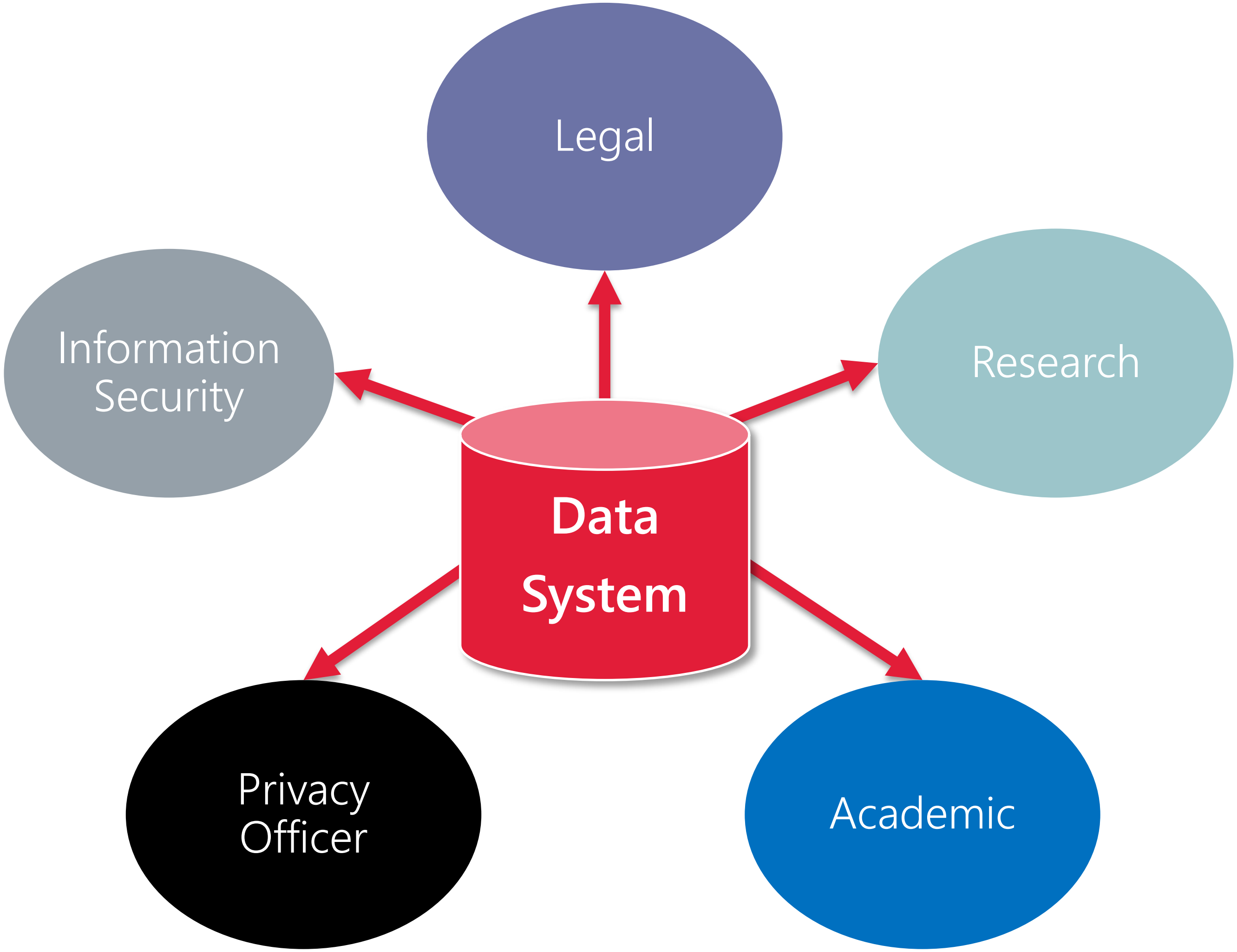
### CUI Basic

- Default, uniform set of standards for handling all categories and subcategories of CUI

### CUI Specified

- Sets of standards that apply to CUI categories and subcategories that have specific handling standards required or permitted by authorizing laws, regulations, or Government-wide policies.

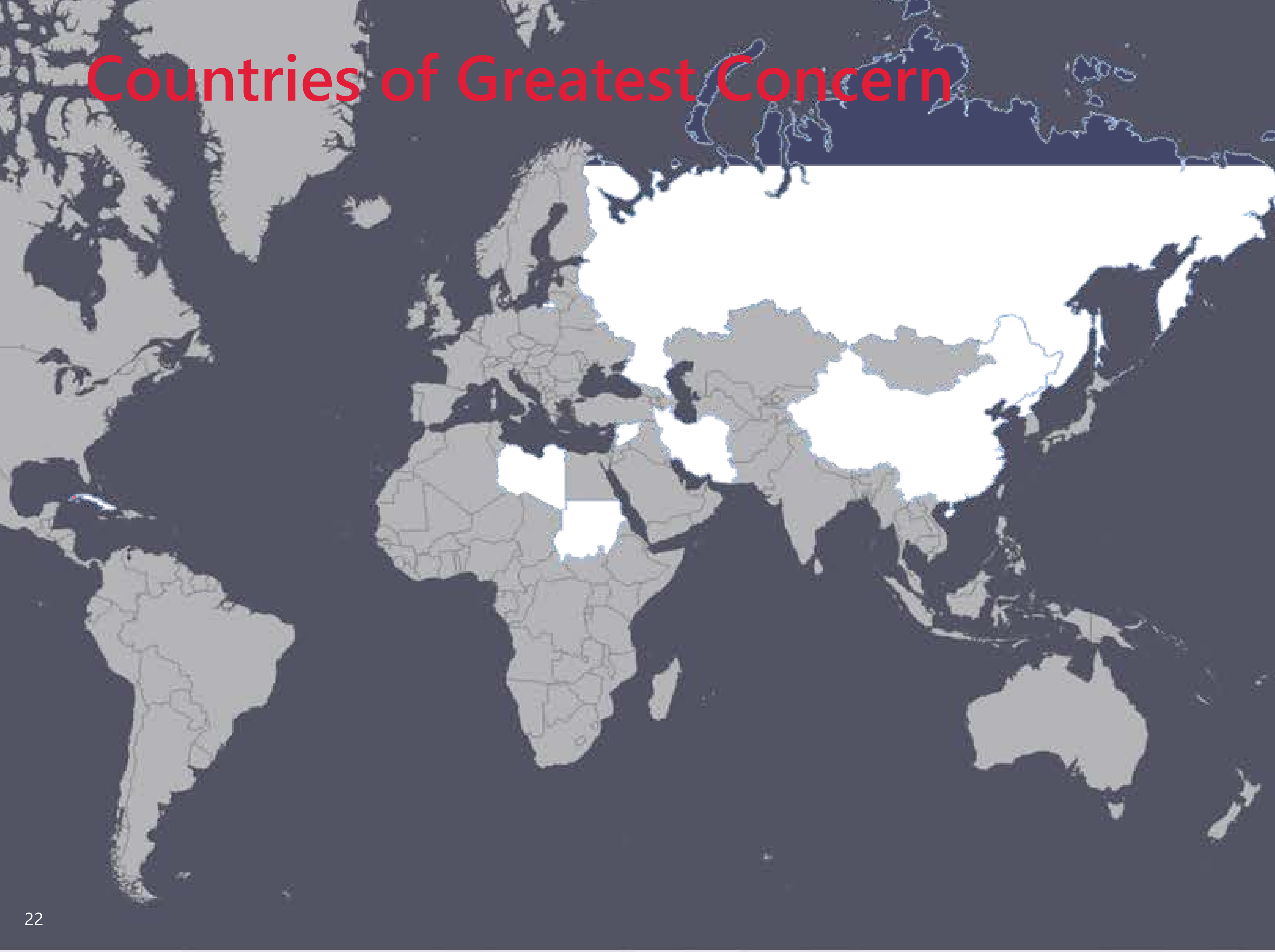
# 7012 Compliance Decision



# 252.239-7010 Cloud Computing Services

# Ancillary Issues

# Countries of Greatest Concern

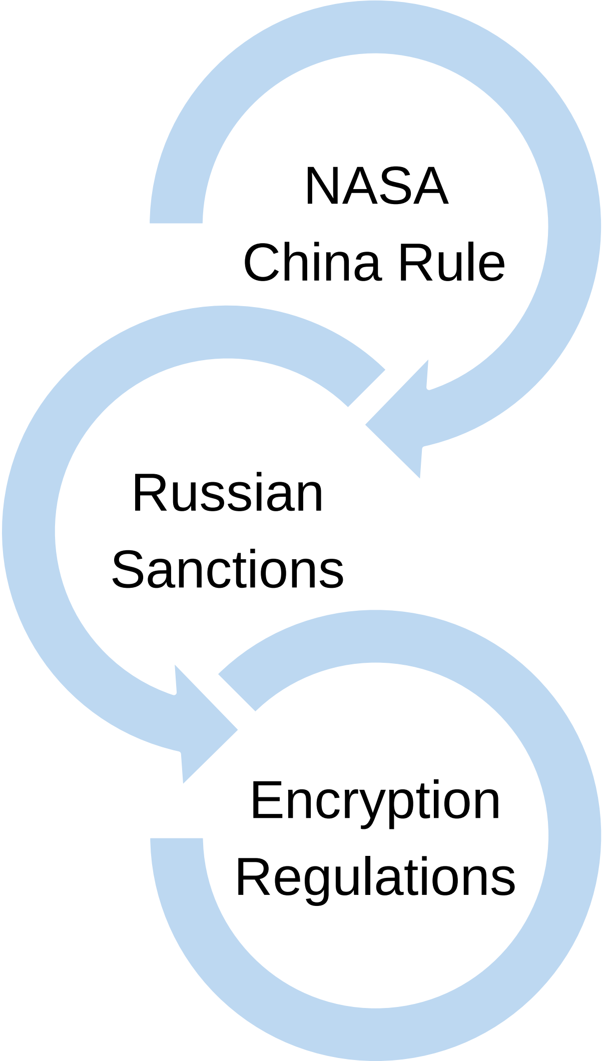


# DD Form 2345 Militarily Critical Technical Data Agreement

## Under the Canada/US Joint Program

- A certification is required by U.S. or Canadian contractors for access to unclassified technical data disclosing militarily critical technology with military or space application that is under the control of, or in the possession of the U.S. Department of Defense (DoD) orthe Canadian Department of National Defence (DND).
- Issued by Defense Logistics Information Services (DLIS)
- Valid for five (5) years
- Must be signed by an authorized official

# Related Regs



NASA China Rule

Russian Sanctions

Encryption Regulations

# Checklist of Good Practices

# 7 Elements of a Good Compliance Program

Establish Policies, Procedures and Controls

Exercise Effective Compliance and Ethics Oversight

Exercise Due Diligence to Avoid Delegation of Authority to Unethical Individuals

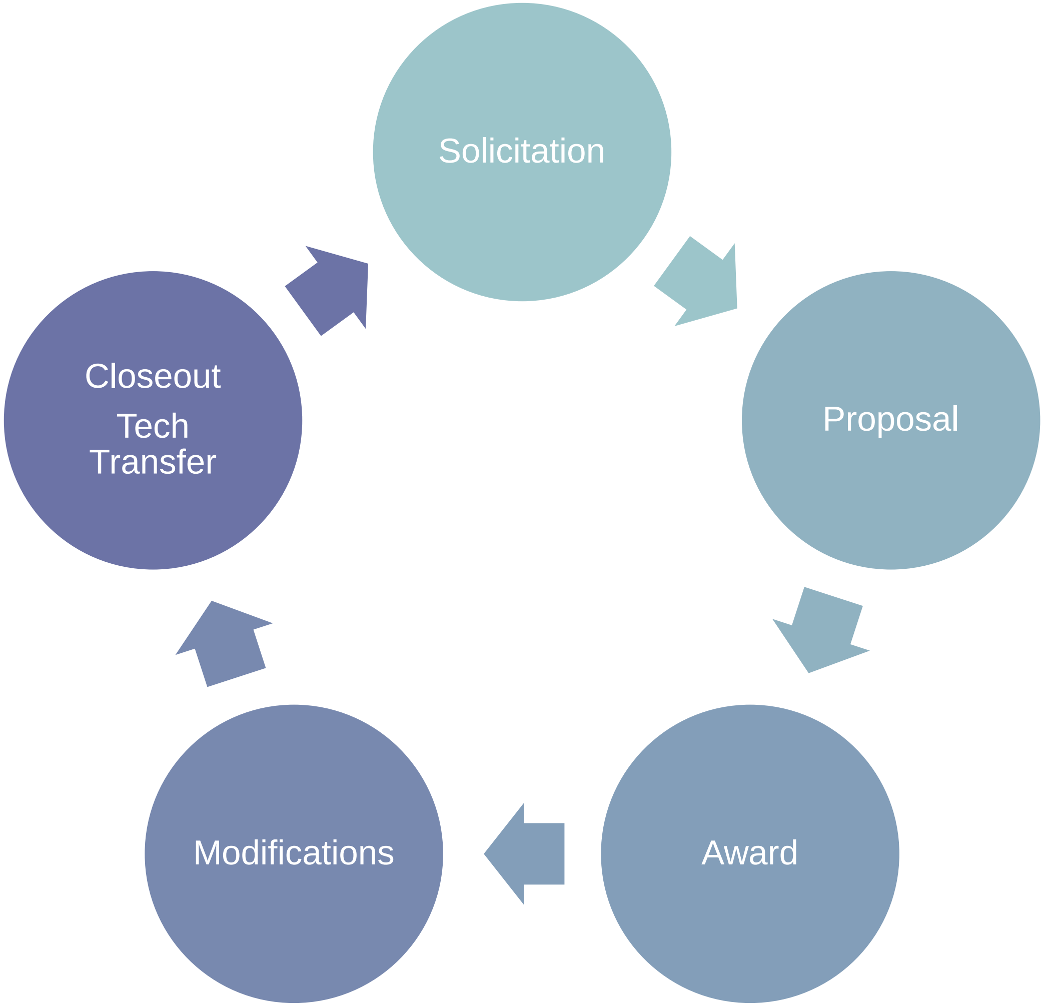
Communicate and Educate Employees on Compliance and Ethics Programs

Monitor and Audit Compliance and Ethics Programs for Effectiveness

Ensure Consistent Enforcement and Discipline of Violations

Respond Appropriately to Incidents and Take Steps to Prevent Future Incidents

# Sponsored Projects



Solicitation

Proposal

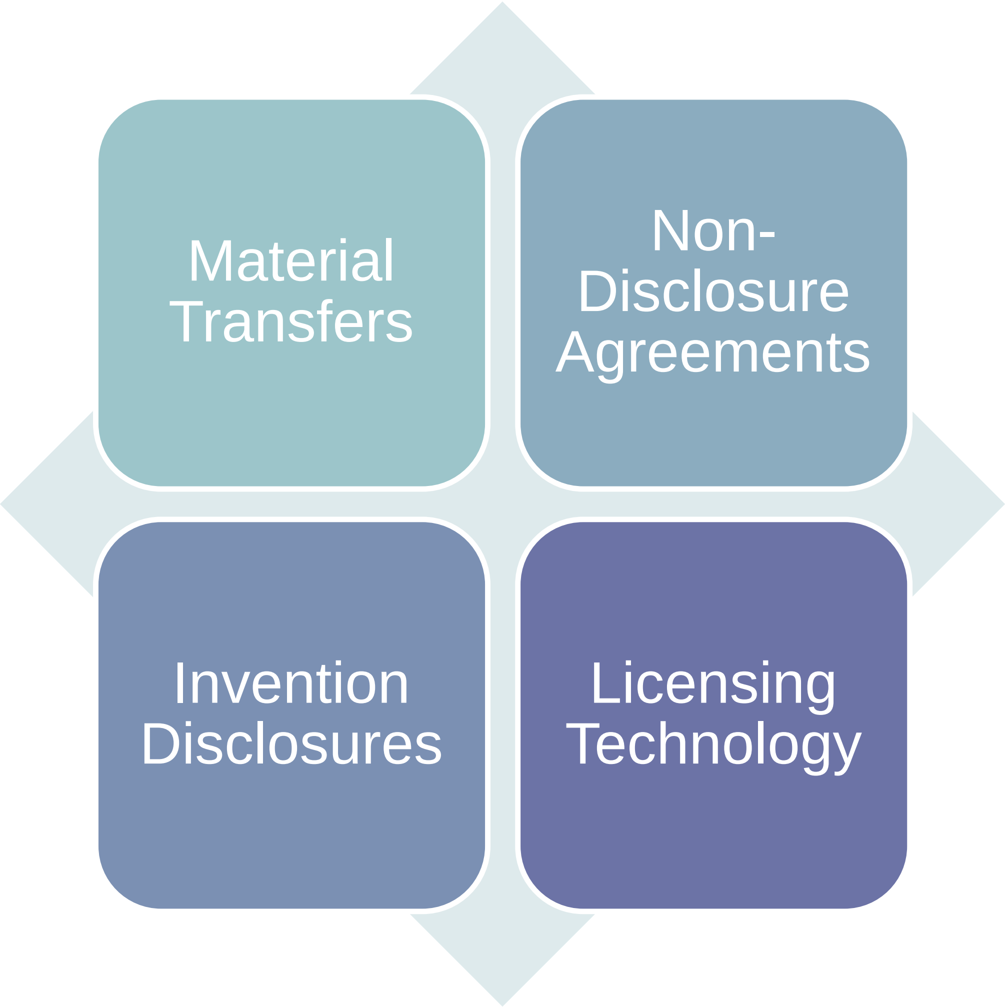
Award

Modifications

Closeout

Tech Transfer

# Technology Transfer

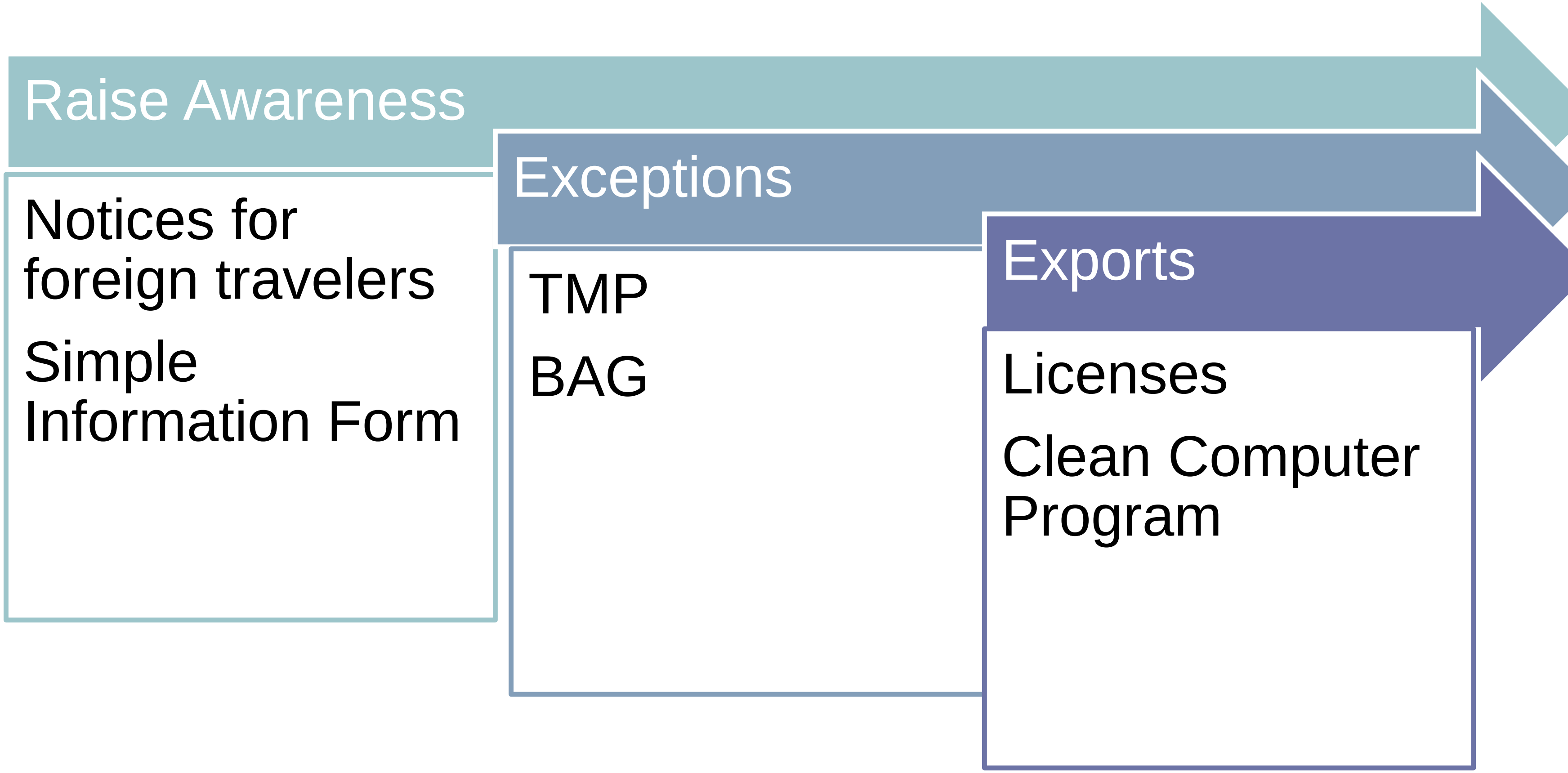

Material Transfers

Non-Disclosure Agreements

Invention Disclosures

Licensing Technology

# Travel



Raise Awareness

Notices for foreign travelers

Simple Information Form

Exceptions

TMP

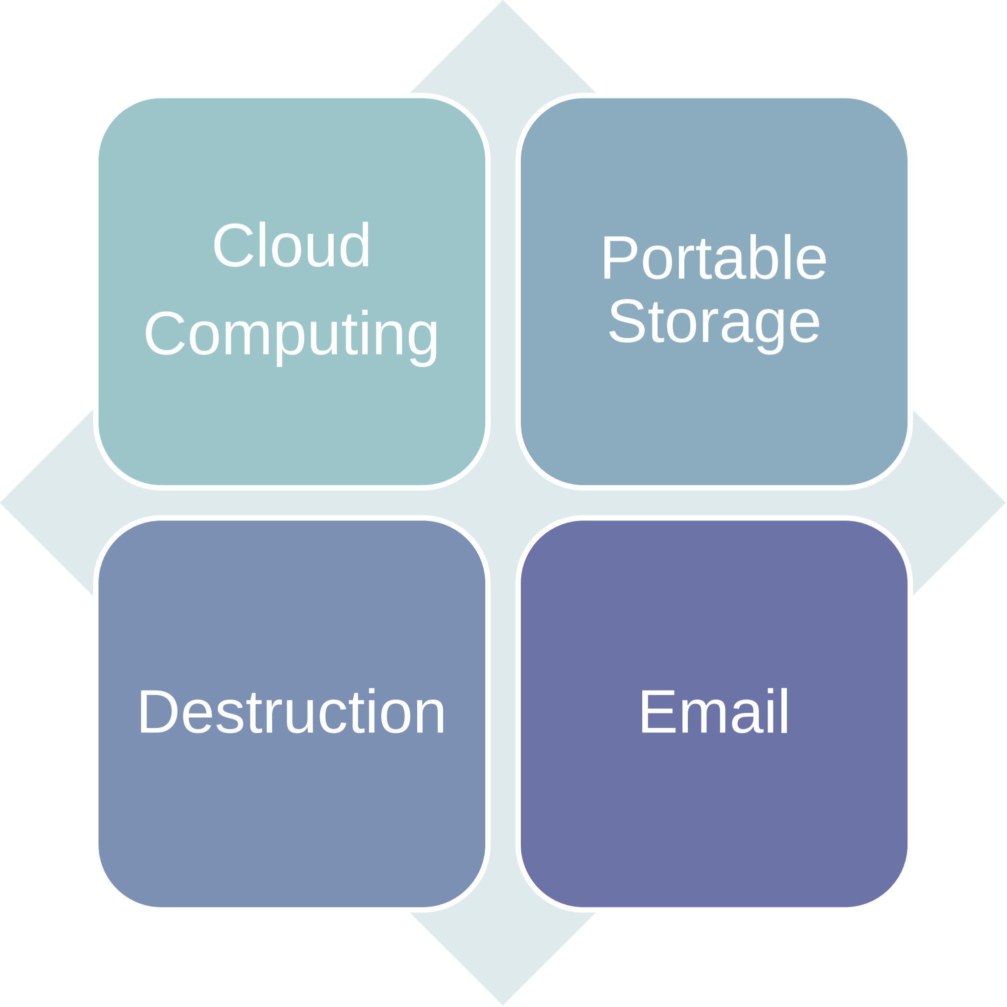
BAG

Exports

Licenses

Clean Computer Program

# Digital Data Concerns



Cloud Computing

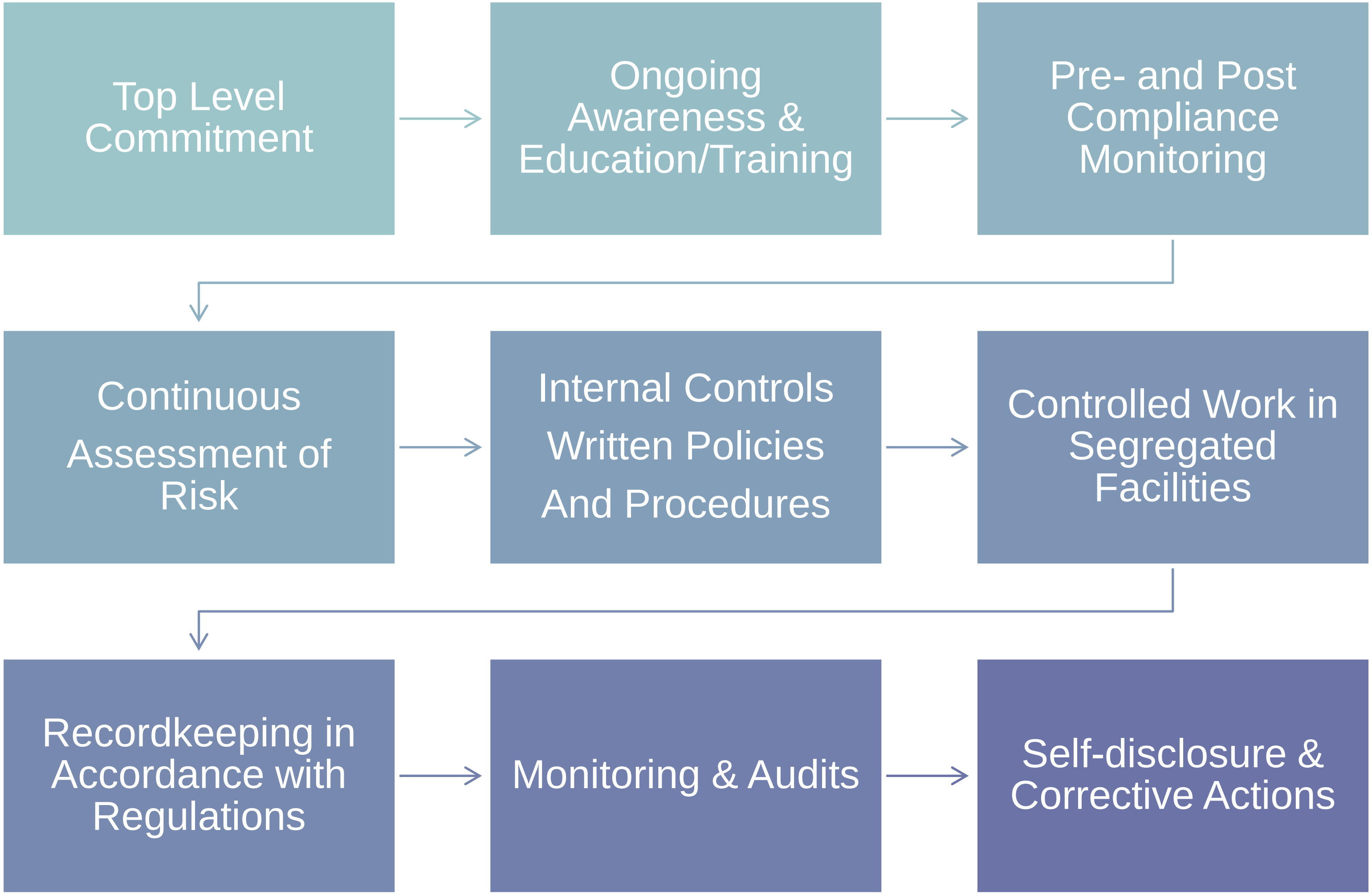
Portable Storage

Destruction

Email

# Assessing the Efficacy of Your Program

# Effective Compliance



Top Level Commitment

Ongoing Awareness & Education/Training

Pre- and Post Compliance Monitoring

Continuous Assessment of Risk

Internal Controls Written Policies And Procedures

Controlled Work in Segregated Facilities

Recordkeeping in Accordance with Regulations

Monitoring & Audits

Self-disclosure & Corrective Actions

# Export Manual Content

## Nunn-Wolfowitz Task Force Report

- Summaries of applicable export laws and regulations
- Charts or diagrams showing the organizational compliance structure
- Policies and procedures regarding export compliance
- Technology classification and license matrices
- Operations and licensing process flow charts
- Sample forms, instructions and agreements
- Contact list of important export compliance employees
- Lists of other export compliance resources

# BIS Elements of Good Compliance

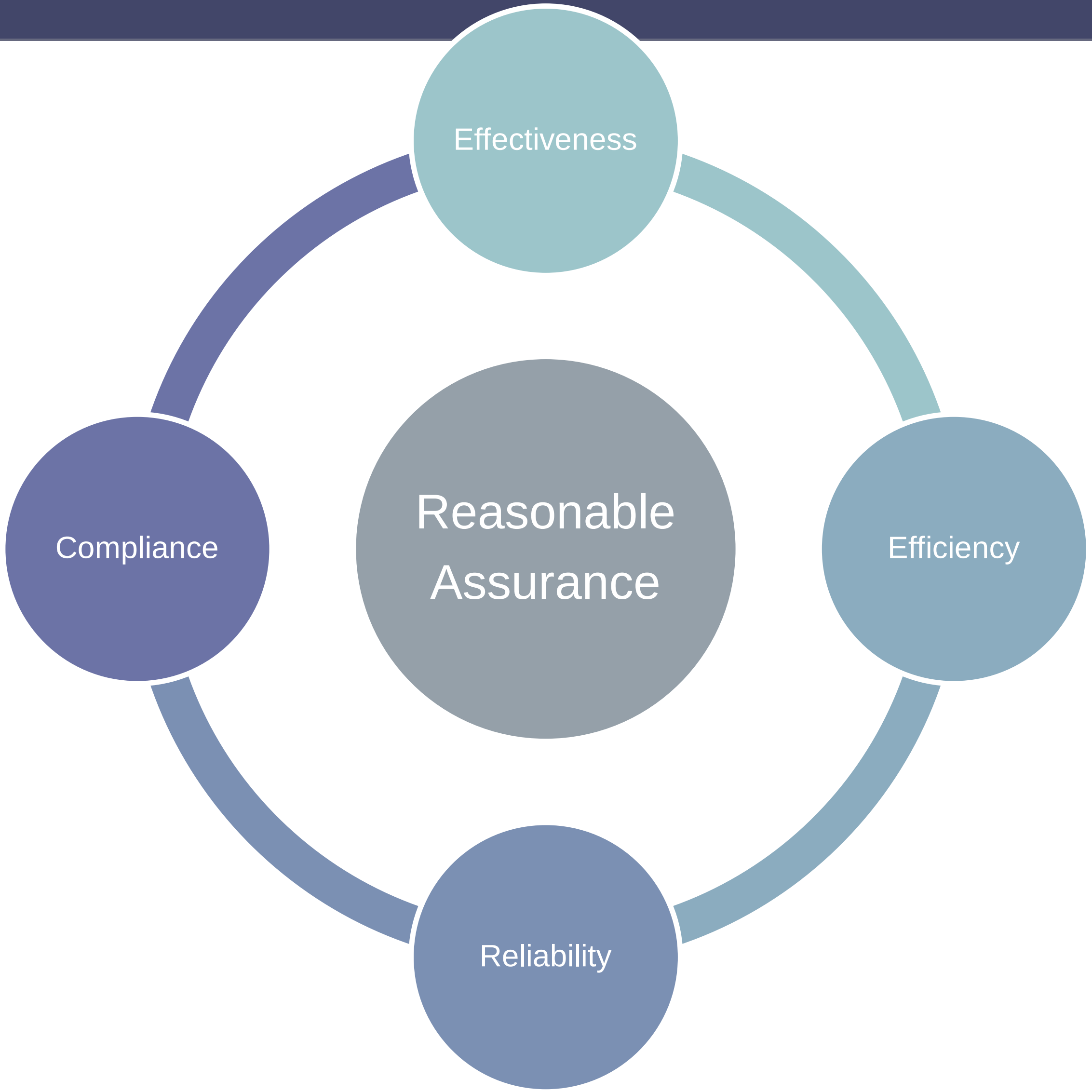
- Management Commitment
- Continuous Risk Assessment of the Export Program
- Formal Written Export Management and Compliance Program
- Ongoing Compliance Training and Awareness
- Pre/Post Export Compliance Security and Screening
- Adherence to Recordkeeping Regulatory Requirements
- Internal and External Compliance Monitoring and Periodic Audits
- Maintaining a Program for Handling Compliance Problems, including Reporting Export Violations
- Completing Appropriate Corrective Actions in Response to Export Violations

# DDTC Required Elements

Effective manuals and programs include:

- Organizational structure
- Corporate commitment policy
- Identification, Receipt and Tracking of ITAR Controlled Items/Technical Data
- Re-Exports/Retransfers
- Restricted/Prohibited Exports and Transfers
- Recordkeeping
- Internal Monitoring
- Training
- Violations and Penalties

# Internal Controls



Effectiveness

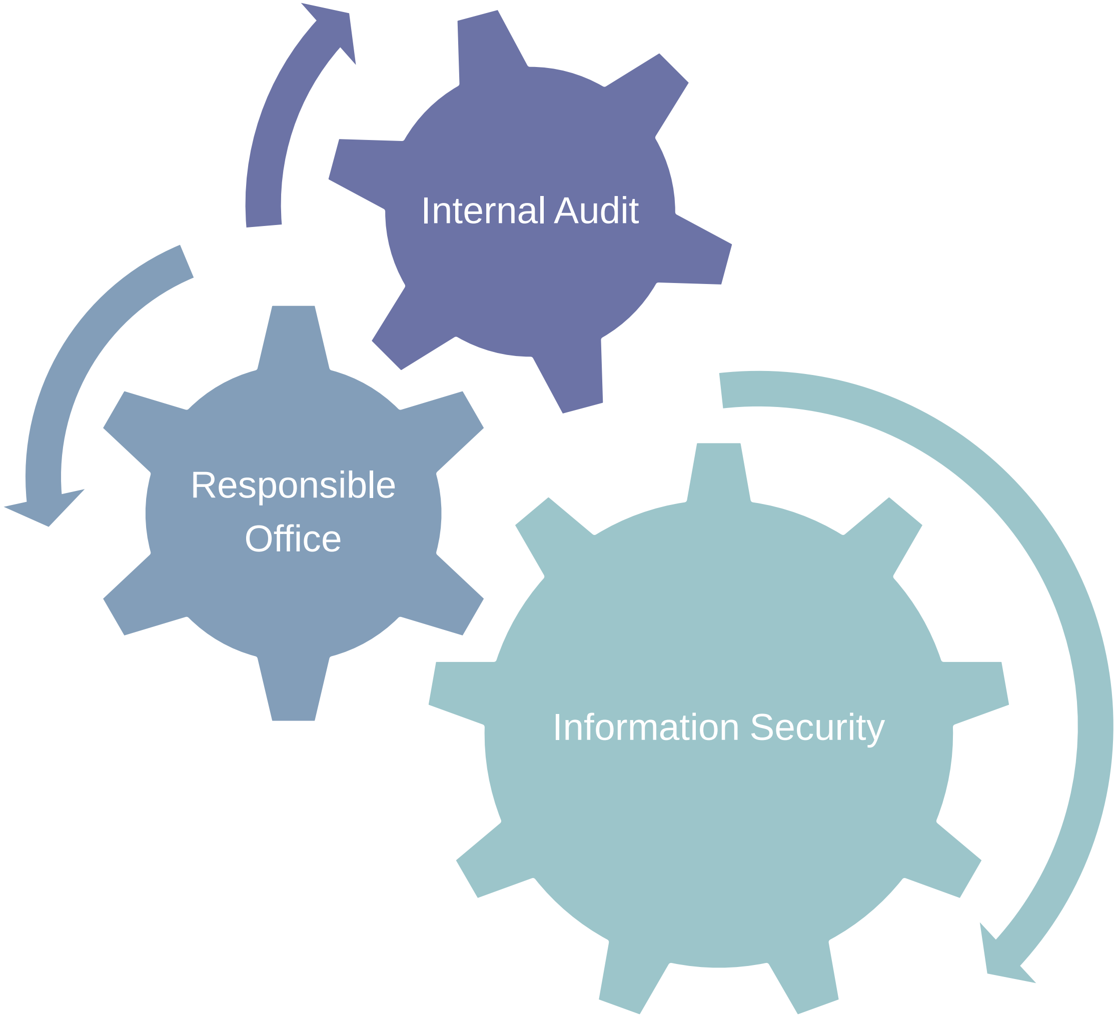
Efficiency

Reliability

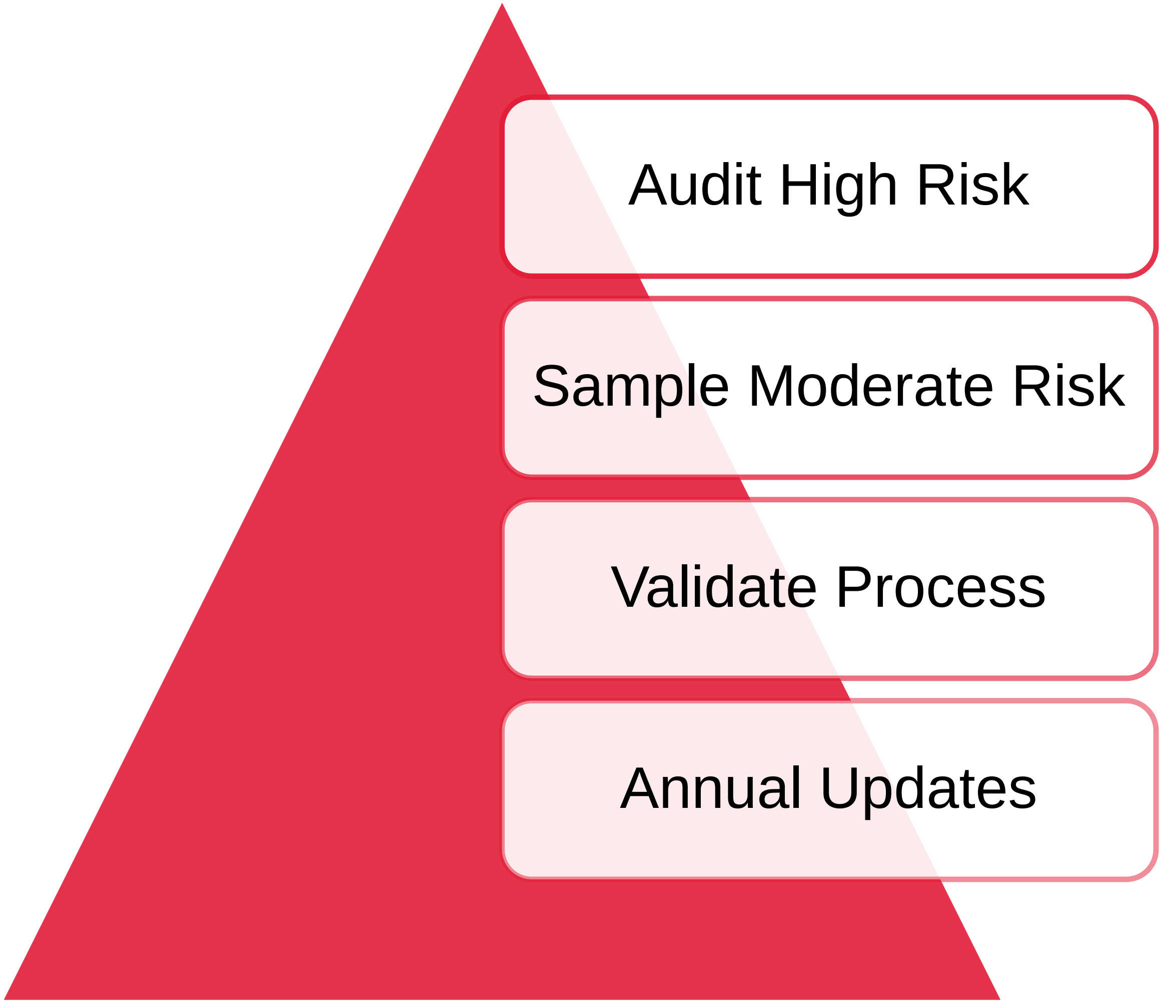
Compliance

Reasonable Assurance

# Assessing Effectiveness



# Audit Sample



Audit High Risk

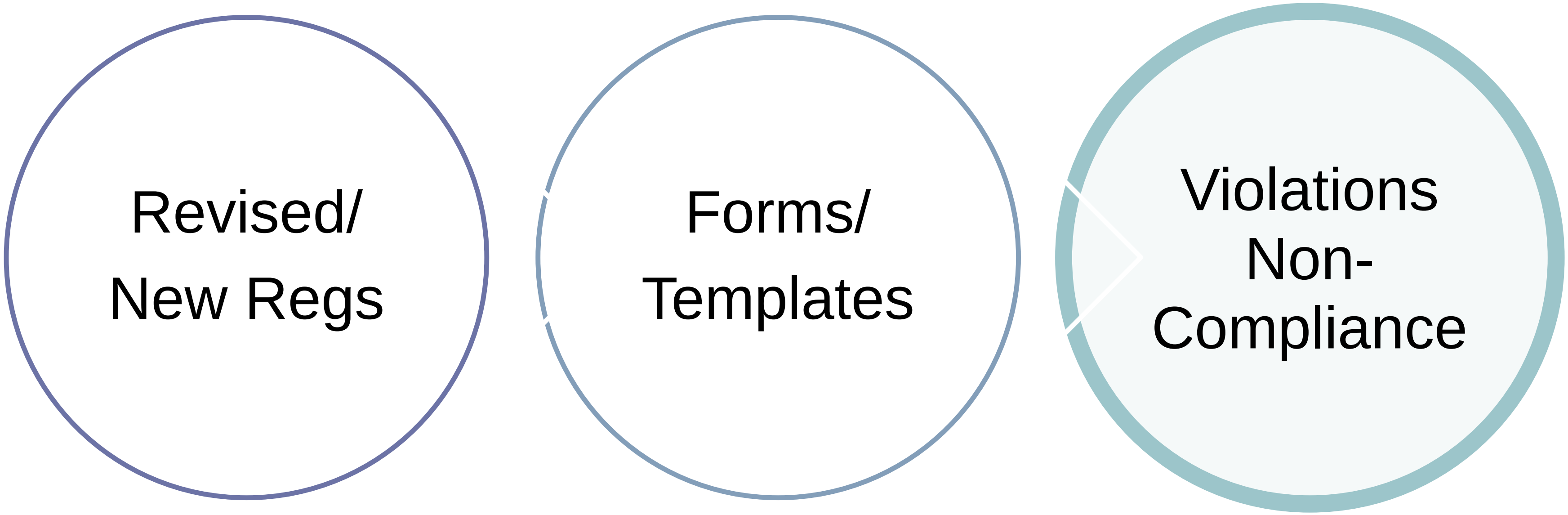
Sample Moderate Risk

Validate Process

Annual Updates

©2015 Attain, LLC

# Periodic Updates of Policies and Procedures



Revised/ New Regs

Forms/ Templates

Violations Non-Compliance

# Dealing with Issues of Non-compliance

# Violations

## Legal Implications

- Civil: Fines and Forfeitures
- Criminal: Fines and Incarceration

## Loss of Export Privileges

## Bad Press

- University of Tennessee
- Temple University

## Voluntary disclosures and compliance efforts mitigate penalties

# Dealing with Potential Violations

## Discovery

- Audits
- Provide a safe environment for reporting
- Have written procedures for handling potential violations

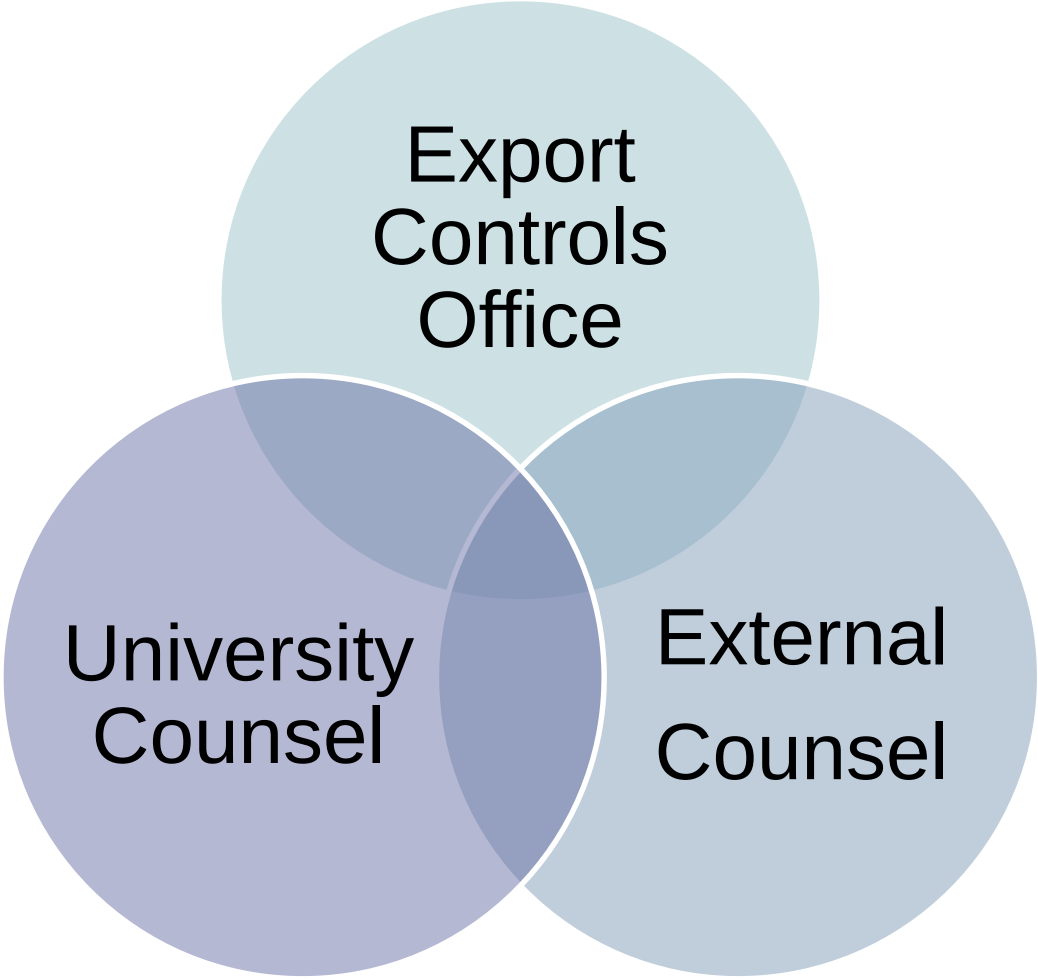
## Investigate

- Provide a timely response
- Ensure compliance is restored
- Inform those on the escalation tree
- Self-report within required timeframe

## Corrective Action

- Determine the cause and accountability
- Revise internal controls, if needed
- Take disciplinary action, if warranted

# Legal Support



Export Controls Office

University Counsel

External Counsel

# Contact Information

**Susan Wyatt Sedwick, PhD, CRA, CSM**
Consulting Associate
Attain, LLC
ssedwick@attain.com
Phone: 512.983.4525