UNCLASSIFIED / APPROVED FOR PUBLIC RELEASE

Program Protection and Exportability

Advancing Today's Training
Defeating Tomorrow's Threats

22 FEB 2024

UNCLASSIFIED / APPROVED FOR PUBLIC RELEASE

BACKGROUND and PURPOSE

Background

- **AR 70-77 Program Protection**, assigns responsibilities and prescribes policies for developing plans to protect *critical program information (CPI)*, conducting supply-chain risk management (SCRM), and performing damage assessment activities resulting from a compromise of unclassified program information.
- Understanding AR 70-77 enables PEO STRI to support the Army's Program Protection requirements for our assigned Programs of Record (including OTA efforts)

Purpose

- Provide a 'high-level' AR 70-77 update to gain an initial awareness of Technology and Program Protection and Responsibilities and understand implications for exportability
- Gain an initial understanding of AR 70-77 requirements including contract implications
- Discuss Industry challenges and best practices with Program Protection and Exportability

U.S. ARMY

Advancing Today's Training
Defeating Tomorrow's Threats

Changes in the Environment

- Increased interconnection of systems
- Increased reliance on Software for system functionality
- Increased complexity of the supply chain

Defense Acquisition System Overarching Policies

DoDD 5000.01

- **Plan for Coalition Partners**. To enable allies and partners to enhance U.S. military capability, collaboration opportunities, potential partnerships, and international acquisition and exportability features and limitations will be considered in the early design and development phase of acquisition programs.
- **Deploy Interoperable Systems**. Joint concepts, standardization, and integrated architectures will be used to the maximum extent possible to characterize the exchange of data, information, materiel, and services to and from systems, units, and platforms to **assure all systems effectively and securely interoperate with other U.S. forces and coalition partner systems**.

DoDI 5000.02

- PMs will consider acquisition strategies that leverage international acquisition and supportability planning to **improve economies of scale, strengthen the defense industrial base, and enhance coalition partner capabilities**.

U.S. ARMY

Advancing Today's Training
Defeating Tomorrow's Threats

Program Protection Policy

1. **Information**
   - Protecting from the threat of malicious insertion into information and communication technology (ICT)
2. **Critical Program Information (CPI)**
   - Identifying and protecting CPI
3. **Trusted Systems and Networks (TSN)**
   - Creating a secure development environment and supply chain
   - Developing a system that is designed to protect, detect, and respond to attacks
   - Implementing protections to ensure mission-critical functions operate as intended

U.S. ARMY

Advancing Today's Training
Defeating Tomorrow's Threats

AR 70-77 Technology and Program Protection

- PEO
  - Establish local policies, procedures, and guidance to ensure program managers (PMs) comply with this regulation and implement adequate program protection plans (PPPs).
- PMs
  - Follow the Department of Defense Technology and Program Protection Guidebook for implementation of program protection planning and execution.
  - Evaluate for CPI and critical technology and employ measures for its protection.
  - PMs will evaluate pursuing exportable versions.

U.S. ARMY

Advancing Today's Training
Defeating Tomorrow's Threats

Program Protection and Foreign Involvement / Design for Export

“Exportability” - The process to identify, develop and integrate technology protection features into U.S. defense systems early in the acquisition process to protect Critical Program Information (CPI) and other critical technologies / capabilities and thus enables a system’s export to partners. Technology protection primarily involves two tools: ***Anti-Tamper (AT) and differential capability modifications***.”

Joint Capability Integration & Development System (JCIDS) Manual (October 2021)

U.S. ARMY

Advancing Today’s Training
Defeating Tomorrow’s Threats

Program Protection and Foreign Involvement / Design for Export

- Two areas under the PPP Addressing Exportability:

1. Section 8.0 Foreign Involvement

    - Foreign Cooperative Development or FMS
    - Safeguarding the sharing of program information with allies
    - Have previous generations of the system been sold to foreign allies?
    - How will export requirements be addressed if a FMS is identified?

Program Protection and Foreign Involvement / Design for Export

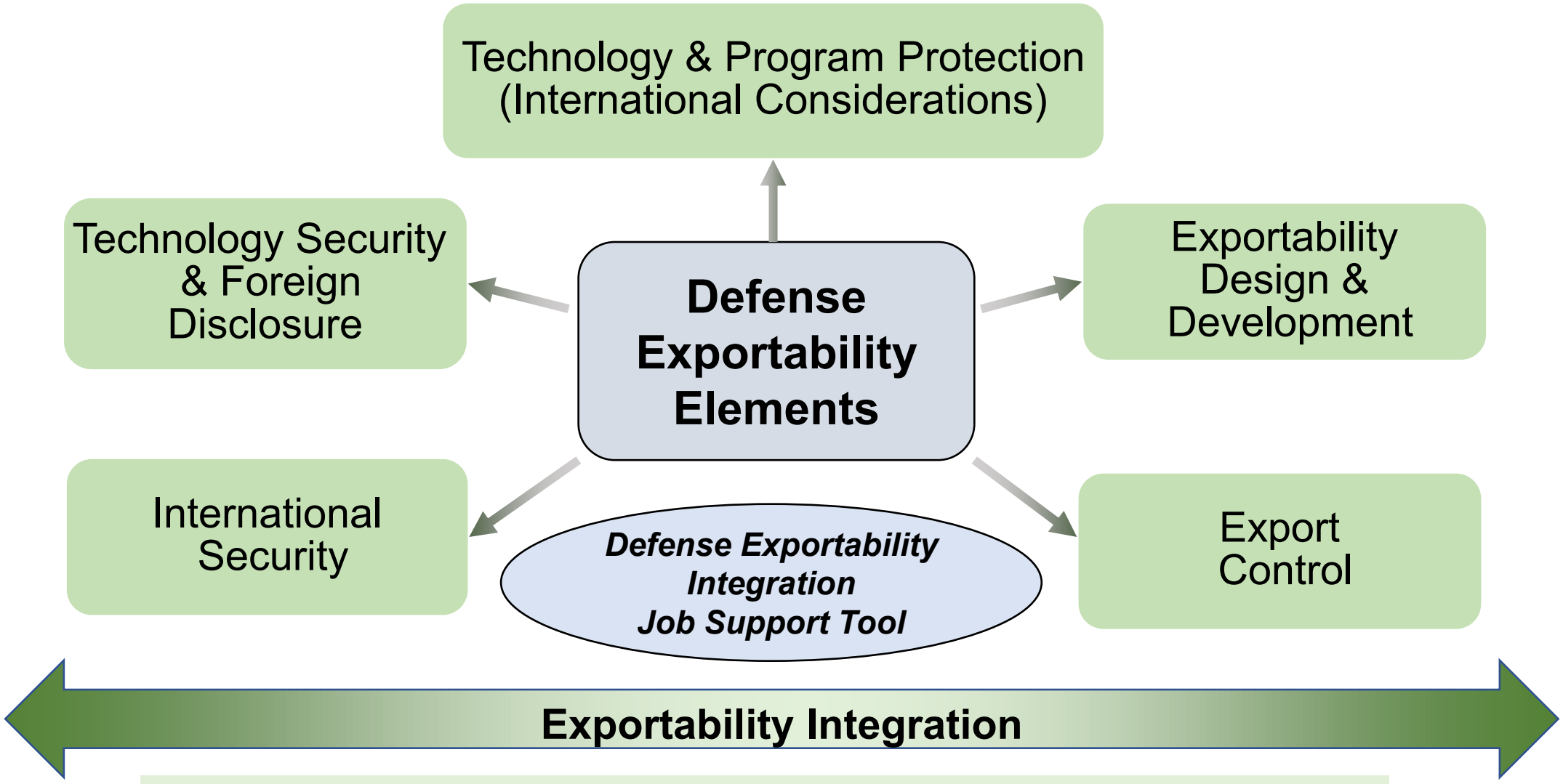
- Two areas under the PPP Addressing Exportability:

2. Section 8.1 Defense Exportability Features

    - What are the impacts and risks to the program from FMS and direct commercial sales?

    - Will the program be a viable Defense Exportability Features (DEF) candidate to develop, plan, and design an export variant during the research and development phase?

Defense Exportability Framework



Address and integrate each element in program level planning

Areas to be considered

- Networked systems
- Software intensive systems – Agile software development
- Supply Chain: Prime integrator, many suppliers (COTS, GOTS and custom)
- Hardware - MOSA
- Data – Enterprise Data Services, traceability of data to the source
- Cybersecurity

Contracting

- New contracts supporting acquisition programs where CPI or ICT critical components have been identified, will contain contractual terms requiring the contractor to implement protection measures.
  - Includes incorporating language in request for proposals that require their defense industrial base partners and all tiers of contractors supporting the system to develop and implement measures for protecting program information on their networks.

TAKE – AWAYS

- **IAW AR 70-77 para 3-9 a: PMs will develop Program Protection plans during R&D and production phases of programs -** Incorporate technology protection features into a system or subsystem to protect US technology and Soldiers

- **PMs will evaluate pursuing exportable versions of the systems as part of the acquisition strategy**

- **Programs may incorporate Anti-Tamper (AT) and differential capability modifications protection mechanisms**

- **Need Industry help with designing systems to allow for exportability**

- **What are the challenges and best practices with Program Protection and Exportability?**

IMPLEMENT FOCUSED EFFORTS TO PREVENT UNAUTHORIZED RELEASE OF TECHNOLOGY AND DATA